Dr.WEB®
Anti-virus
for Windows

Defend what you create

User Manual

© Doctor Web, 2003-2011. All rights reserved.

This document is the property of Doctor Web. No part of this document may be reproduced, published or transmitted in any form or by any means for any purpose other than the purchaser's personal use without proper attribution.

TRADEMARKS
Dr.Web, the Dr.WEB logo, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-desk are trademarks and registered trademarks of Doctor Web in Russia and/or other countries. Other trademarks, registered trademarks and company names used in this document are property of their respective owners.

DISCLAIMER
In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

Dr.Web® Anti-virus For Windows
Version 6.0
User Manual
11.08.2011

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Refer to the official web site for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web® information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards. State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of Contents

Introduction 7

- **What is This Manual About** 9
- **Document Conventions and Abbreviations** 10
- **System Requirements** 11
- **Licensing** 12
  - Key File 12
  - Get Key File 13
  - Renewing registration 15
- **How to Test Anti-virus** 17
- **Detection Methods** 18

Installing Dr.Web Anti-virus 20

- **Installation procedure** 21
- **Reinstalling and Removing Dr.Web Anti-virus** 32

Receiving the Key File 34

Getting Started 36

- **SpIDer Agent** 38
  - SpIDer Agent Settings 41
- **License Manager** 44
- **Quarantine** 46
- **Using Dr.Web Scanner for Windows** 49
  - Launching Scanner. General Information. 50
  - Actions Upon Detection of a Virus 54
  - Adjusting Scanner Settings 57

Command Line Scanning Mode 62
DWScancl Console Scanner 64
SpIDer Guard for Windows 65
Managing the Guard 66
Main Parameters of the SpIDer Guard 67
SpIDer Mail 72
Managing SpIDer Mail 74
Adjusting Certain Program Settings 75
Dr.Web for Outlook 80
Virus Check 82
Logging 85
Statistics 87
Dr.Web Firewall 88
Training Dr.Web Firewall 88
Managing Dr.Web Firewall 95
Firewall settings 97
Event Logging 121
Automatic Launch of Tasks for Scanning and Updating in Dr.Web 127
Automatic Updating 130
General Information 130
Launching and Using the Automatic Updating Utility 133
Appendices 137
Appendix A. Additional Command Line Parameters of the Anti-virus 137
Appendix B. Adjustable Parameters of Dr.Web Components 151

Appendix C. Malicious Programs and Methods of Neutralizing Them 168

Appendix D. Naming of Viruses 175

Appendix E. Corporate network protection by Dr.Web® Enterprise Suite 180

Appendix F. Dr.Web® AV-Desk for Internet services providers 187

Appendix G. Technical Support 192

Introduction

Dr.Web® Anti-virus For Windows provides multi-level protection of RAM, hard disks and removable devices against viruses, rootkits, Trojans, spyware, adware, hack tools and other malicious programs. The module architecture of **Dr.Web Anti-virus** is its significant feature. **Dr.Web** uses the anti-virus engine and virus databases which are common for all its components and different operating environments. At present, in addition to **Dr.Web Anti-virus**, there are versions of the anti-virus for IBM® OS/2®, Novell® NetWare®, Macintosh®, Microsoft Windows Mobile®, Andorid®, Symbian® and several Unix®-based systems (Linux®, FreeBSD®, Solaris®).

Dr.Web is designed as a powerful anti-virus program and regularly shows the best results in independent comparative reviews.

Dr.Web uses a convenient and efficient procedure for updating the virus database and program components via the Internet.

Dr.Web can detect and remove undesirable programs (adware, dialers, jokes, riskware, and hacktools) from your computer. For detection of undesirable programs and actions with the files contained in them, standard anti-virus components of **Dr.Web** are used.

Dr.Web Anti-virus includes the following components:

- **Dr.Web Scanner for Windows** (**Scanner**) is an anti-virus scanner with graphical interface. The program is run on user demand or according to schedule, and checks the computer for viruses. There is also a command line version (**Dr.Web Console scanner for Windows**).
- **SpIDer Guard® for Windows** (also called **Monitor** or **Guard**) is an anti-virus guard. The program resides in main memory, checks files and memory on the fly, and detects virus-like activity.
- **SpIDer Mail® for Windows** (**Mail Guard**) is a mail anti-virus guard. The program intercepts calls sent from mail clients to mail servers through POP3/SMTP/IMAP4/NNTP protocols (IMAP4 stands for IMAPv4rev1), detects and neutralizes mail

viruses before a mail message is received by the mail client, or before a mail message is sent to the mail server.

- **Dr.Web for Outlook** is a plug-in that checks Microsoft Outlook mail boxes for viruses.
- **Dr. Web Firewall** protects your computer from unauthorized access and prevents leak of vital data through networks.
- **Dr.Web Automatic Updating Utility for Windows** (**Updater**) allows registered users to receive updates of the virus database and other files of the program, as well as automatically install them. Moreover, the **Updater** lets registered users renew their license (serial number is required). For unregistered users it allows to register and receive a license or demo key file (see Receiving the Key File chapter).
- **SpIDer Agent** is a utility which lets you set up and manage components of **Dr.Web**.

To centralize the management of the anti-virus protection at an enterprise level, a special program – **Dr.Web Enterprise Suite** – is supplied. For more details on this program read Appendix E.

Internet service providers can organize anti-virus and anti-spam protection of their clients using **Dr.Web AV-Desk**. For more information on this software see Appendix F.

What is This Manual About

This User Manual describes installation and effective utilization of **Dr.Web Anti-virus**.

You can find detailed description of all the GUI elements in the Help system of **Dr.Web Anti-virus** which can be accessed from any component.

This User Manual describes installation of **Dr.Web Anti-virus** and contains some words of advice on how to use the program and solve typical problems caused by virus threats. Mostly, it describes standard operating modes of the program's components (with default settings).

The Appendices contain detailed information for experienced users on how to set up **Dr.Web Anti-virus**.

In connection with constant development, the program interface can mismatch the images given in this document. You can always find the actual help information on http://products.drweb.com.

Document Conventions and Abbreviations

The following symbols and text conventions are used in this guide:

Convention	Description
Bold	Names of buttons and other elements of the graphical user interface (GUI), and required user input that must be entered exactly as given in the guide.
Green and bold	Names of **Dr.Web** products and components.
Green and underlined	Hyperlinks to topics and web pages.
`Monospace`	Code examples, input to the command line and application output.
Italic	Placeholders which represent information that must be supplied by the user. For command-line input, it indicates parameter values. In addition, it may indicate a term in position of a definition.
CAPITAL LETTERS	Names of keys and key sequences.
Plus sign ('+')	Indicates a combination of keys. For example, ALT+F1 means to hold down the ALT key while pressing the F1 key.
Exclamation mark	A warning about potential errors or any other important comment.

The following abbreviations are used in this User Manual:

- GUI – Graphical User Interface (GUI-version of program - a version which utilizes the GUI)
- OS – operating system
- PC – personal computer
- RAM – Random Access Memory

System Requirements

Before installing **Dr.Web Anti-virus**, you should:

- install all critical updates recommended by the OS developer;
- uninstall all other anti-virus packages from the computer to avoid possible incompatibility with their resident components;
- if you install **Dr.Web Firewall**, uninstall all other firewalls.

Specification	Requirement
OS	One of the following: • Microsoft® Windows® 2000 Workstation SP4 with Update Rollup 1 • Windows® XP SP2 • Windows® Vista • Microsoft® Windows® 7 Both 32-bit and 64-bit versions of operating systems are supported. You may need to download and install certain system components from the official Microsoft Web site. If necessary, the program will notify you about the components required and provide download links.
Hard disk space	Minimum 250 MB of disk space for a full installation, which includes: • Up to 70 MB of installation files • Up to 90 MB of temporary setup files that are removed automatically at completion of install
CPU	i686 compatible
RAM	512 MB and more
Other	Internet connection for updating of virus databases and **Dr.Web Anti-virus** components.

Licensing

The use rights for the **Dr.Web Anti-virus** are specified in the key file.

To use **Dr.Web Anti-virus**, obtain and install a key file.

For more information on licensing and types of key files, visit the official Doctor Web website.

Key File

The key file contains the following information:

- list of components a user is allowed to use
- duration of the license
- other restrictions (for example, the number of computers on which a program is allowed to be used on)

The key file has the .key extension and, by default, should reside in the installation folder of the program.

The key file has a write-protected format and must not be edited. Editing the key file makes it invalid. Therefore, it is not recommended to open your key file with a text editor which may accidentally corrupt it.

There are three types of key files:

- *License key file* is purchased with the **Dr.Web** software and allows a user to use it and receive technical support. Parameters of the license key file are set in accordance with the software's license agreement. It also contains information about the user and seller.
- *Demo key file* is used for evaluation of **Dr.Web** products. It is completely free, provides full functionality of the software, but

has a limited duration – 30 days.

Demo key files for the same computer cannot be received more often then once in 4 months.

- *Temporary key file* is used if you do not install licence or demo key file during installation. This key file provides full functionality of **Dr.Web Anti-virus** components, however updating is not available until you install licence or demo key file.

A *valid* license key file satisfies the following criteria:

- License is not expired
- All anti-virus components required by **Dr.Web Anti-virus** are licensed
- Integrity of the license key file is not violated

If any of the conditions are violated, the license key file becomes *invalid* and **Dr.Web Anti-virus** stops detecting and neutralizing malicious programs and transmits.

Get Key File

The key file can be delivered as a .key file, or an archive containing such file.

You can receive key files in one of the following ways:

- During installation, first update or later
- Via manual product registration on the official Doctor Web website
- Within the product distribution kit
- On a separate data carrier provided by the seller

Key files received during installation or within installation kit are installed automatically. You need to install key files received in another way.

To acquire key files via manual registration

To register and download key files, a valid Internet connection is required.

To receive a license key file, a product serial number is required. Without a serial number, you can only receive a demo key file during installation.

1. Launch an Internet browser and go to the site specified on the product registration card supplied with your copy of the product.
2. Fill in the registration form.
3. Enter the serial number which is typed on the registration card.
4. The license key file is archived and sent to the e-mail address you specified in the registration form. After registration, you can also download the license key file from the registration page. Windows operating systems extract files from ZIP-archives automatically. You do not need to purchase or install additional software.
5. Install the key file.

To acquire key files during installation

The key file can be delivered as a .key file, or an archive containing such file. A user can receive the key file via the **Dr.Web Updater** after registration during installation or the first update. The utility registers the program (after providing the serial number) on the official web site and receives the key file. This procedure is available only for **Dr.Web** programs which protect individual workstations. Without a serial number the user can only receive a demo key file. (See Receiving key file).

It is required to reboot system after key file is received.

It is recommended to keep the key file until it expires. If you re-install

a product or install it on several computers, additional registration of the serial number will not be required because the key file received during the first registration can be used.

Demo key file can be used only on that computer, where it was registered.

Subsequent Registration

If a key file is lost, you should register again. In this case, input the personal data which you provided during the previous registration. You may use a different e-mail address. In this case, the key file will be sent to the address specified.

When recovering demo key file, you will receive the same key file as you received during the previous registration.

The number of requests for a key file receipt is limited. One serial number can be registered not more than 25 times. If more requests are sent, the key file will not be delivered. In this case, to receive a lost key file, contact Technical Support describing your problem in detail, stating your personal data input during the registration and the serial number.

If no valid key file is found (license or demo), the functionality of the program is blocked.

Renewing registration

When license expires or security of your system is reinforced, you may need to update the license. The new license then should be registered with the product. **Dr.Web Anti-virus** supports hot license update without stopping or reinstalling the product.

To renew license key files

1. Open License Manager. To purchase a new license or renew an existing one, you can also use your personal web page on the **Doctor Web** web site. To visit your page, use **My Dr.Web** option in the **License Manager** or SpIDer Agent menu.
2. If current key file is invalid, **Dr.Web Anti-virus** automatically switches to using the new license.

How to Test Anti-virus

The EICAR (European Institute for Computer Anti-Virus Research) Test File helps testing performance of anti-virus programs that detect viruses using signatures.

For this purpose, most of the anti-virus software vendors generally use a standard test.com program. This program was designed specially so that users could test reaction of newly-installed anti-virus tools to detection of viruses without compromising security of their computers. Although the test.com program is not actually a virus, it is treated by the majority of anti-viruses as if it were a virus. On detection of this "virus", **Dr.Web® Anti-virus For Windows** reports the following: `EICAR Test File (Not a Virus!)`. Other anti-virus tools alert users in a similar way.

The test.com program is a 68-byte COM-file that prints the following line on the console when executed: EICAR-STANDARD-ANTIVIRUS-TEST-FILE!

The test.com file contains the following character string only:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

To create your own test file with the "virus", you may create a new file with this line and save it with as test.com.

In optimal mode **SpIDer Guard** does not detect EICAR file as malicious software, because this file is a DOS application and does not compromise security of computer.

Detection Methods

The **Dr.Web anti-virus solutions** use several malicious software detection methods simultaneously, and that allows them to perform thorough checks on suspicious files and control software behaviour:

1. The scans begin with *signature analysis*, which is performed by comparison of file code segments to the known virus signatures. A signature is a finite continuous sequence of bytes which is necessary and sufficient to identify a specific virus. To reduce the size of the signature dictionary, the **Dr.Web anti-virus solutions** use signature checksums instead of using complete signature sequences. Checksums uniquely identify signatures which preserves correctness of virus detection and neutralization. The **Dr.Web virus databases** are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.
2. On completion of signature analysis, the **Dr.Web anti-virus solutions** use the unique **Origins Tracing™** method to detect new and modified viruses which use the known infection mechanisms. Thus the **Dr.Web** users are protected against such viruses as notorious blackmailer Trojan.Encoder.18 (also known as gpcode). In addition to detection of new and modified viruses, the **Origins Tracing** mechanism allowed to considerably reduce the number of false triggering of the **Dr.Web** heuristics analyser.
3. The detection method used by the *heuristics analyser* is based on certain knowledge about attributes that characterize malicious code. Each attribute or characteristic has weight coefficient which determines the level of its severity and reliability. Depending on the sum weight of a file, the heuristics analyzer calculates the probability of unknown virus infection. As any system of hypothesis testing under uncertainty, the heuristics analyser may commit type I or type II errors (omit viruses or raise false alarms).

While performing any of the abovementioned checks, the **Dr.Web anti-virus solutions** use the most recent information about known malicious software. As soon as experts of **Doctor Web Virus**

Laboratory discover new threats, the update for virus signatures, behaviour characteristics and attributes is issued. In some cases updates can be issued several times per hour. Therefore even if a brand new virus passes through the **Dr.Web resident guards** and penetrates the system, then after update the virus is detected in the list of processes and neutralized.

Installing Dr.Web Anti-virus

Before installing the program we strongly recommend to:

- install all critical updates released by Microsoft for the OS version used on your computer (they are available at the company's updating web site at http://windowsupdate.microsoft.com);
- check the file system with the system utilities and remove the detected defects;
- close all active applications.

Dr.Web Anti-virus is not compatible with other anti-virus software. Installing two anti-virus programs on one computer may lead to system crash and loss of important data.

To begin the installation of **Dr.Web Anti-virus** on your computer, do one of the following:

- Execute the file, if supplied as a single executable file.
- Insert the company disk into the CD/DVD drive. If autorun is enabled, installation procedure will start automatically. If autorun is disabled, run the executable file of the distribution kit manually.

Follow the dialog windows of the installation wizard. At any stage of the installation (before the files are copied onto the computer) you can return to previous stage by clicking **Back**. To continue installation, click **Next**. To abort installation, click **Cancel**.

Installation procedure

Only a user with administrator privileges can install **Dr.Web Anti-virus**.

There are two modes of the installation of **Dr.Web Anti-virus**:

1. The background mode.
2. The usual mode.

Installation in the background mode

To install **Dr.Web Anti-virus** in the background mode, in the command line enter the executable file name with necessary parameters (these parameters affects logging, reboot after installation and **Dr.Web Firewall** installation).

Installation	Parameters
No reboot. No logging.	`/S /V/qn`

Reboot. No logging.	`/S /V"/qn REBOOT=Force"`
	or
	`/S /V"/qn REBOOT=F"`

No reboot. Logging.	`/S /V"/qn /lv* \" <path>\drweb-setup.log\""`

Reboot. Logging.	`/S /V"/qn /lv* \"<path>\drweb-setup.log\" REBOOT=F"`
	or
	`/S /V"/qn /lv* \" <path>\drweb-setup.log\" REBOOT=Force"`

Dr.Web Firewall installation. Reboot.	`/S /V"/qn INSTALL_FIREWALL=1 REBOOT=F"`
	or
	`/S /V"/qn INSTALL_FIREWALL=1 REBOOT=Force"`

For example, to perform installation of **Dr.Web Anti-virus** with logging and reboot after installation, execute the following command:

```
C:\Documents and Settings\drweb-600-win-x86.exe
/S     /V"/qn     /lv*     \"%temp%\drweb-setup.
log\"REBOOT=F"
```

If particular language of the installation is required, use the following additional parameter:

`/L<`*language_code*`>`

For example,

```
/L1049 /S /V"/qn REBOOT=Force"
```

The list of languages:

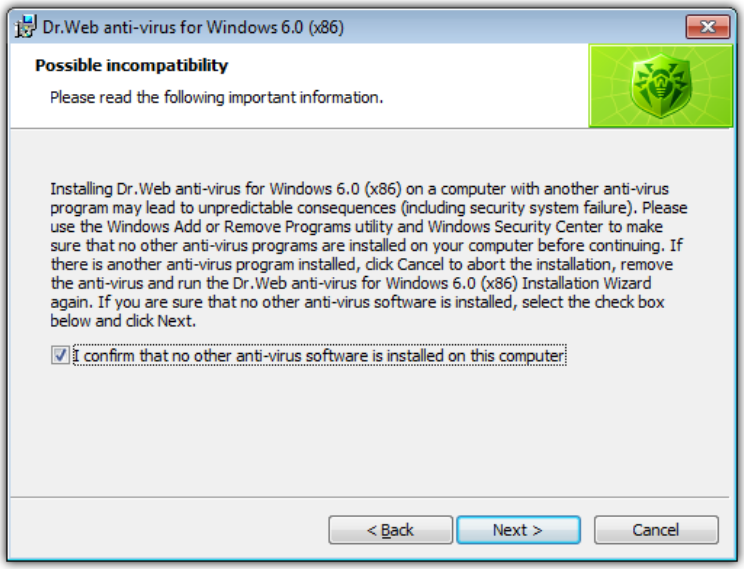
Code	Language
1026	Bulgarian
2052	Chinese (Simplified)
1028	Chinese (Traditional)
1033	English
1061	Estonian
1036	French (France)
1031	German
1032	Greek
1038	Hungarian
1040	Italian
1062	Latvian
1063	Lithuanian
1045	Polish
2070	Portuguese
1049	Russian
1051	Slovak

Code	Language
1034	Spanish (Traditional Sort)
1055	Turkish
1058	Ukrainian

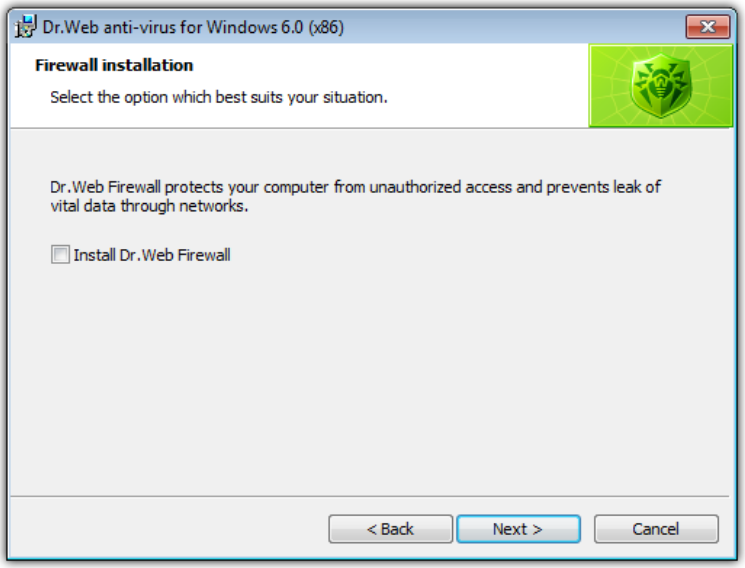
Regardless of your choice English language will be installed in addition.

Installation in the usual mode

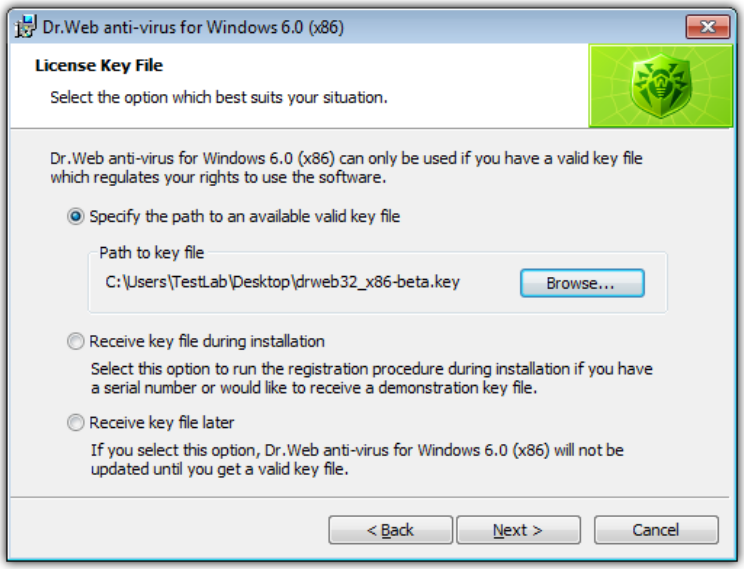
1. Select the language for the installation wizard. Regardless of your choice English language will be installed in addition.
2. In the next window you will be offered to read the License agreement. You should accept it and click **Next** in order to continue installation.
3. The installation wizard will inform on possible incompatibility of **Dr.Web** with other anti-viruses installed on your computer and offer to uninstall or disable them. If other anti-viruses are installed on your computer, it is recommended to click **Cancel** and terminate installation, delete or deactivate other anti-viruses and after that continue installation.
   To continue installation select the **I confirm that no other anti-virus software is installed on this computer** check box and click **Next**.


Dr.Web anti-virus for Windows 6.0 (x86)
Possible incompatibility
Please read the following important information.
Installing Dr.Web anti-virus for Windows 6.0 (x86) on a computer with another anti-virus program may lead to unpredictable consequences (including security system failure). Please use the Windows Add or Remove Programs utility and Windows Security Center to make sure that no other anti-virus programs are installed on your computer before continuing. If there is another anti-virus program installed, click Cancel to abort the installation, remove the anti-virus and run the Dr.Web anti-virus for Windows 6.0 (x86) Installation Wizard again. If you are sure that no other anti-virus software is installed, select the check box below and click Next.
I confirm that no other anti-virus software is installed on this computer
< Back
Next >
Cancel

4. In the next window you will be offered to install **Dr.Web Firewall**.


Dr.Web anti-virus for Windows 6.0 (x86)
Firewall installation
Select the option which best suits your situation.
Dr.Web Firewall protects your computer from unauthorized access and prevents leak of vital data through networks.
Install Dr.Web Firewall
< Back
Next >
Cancel

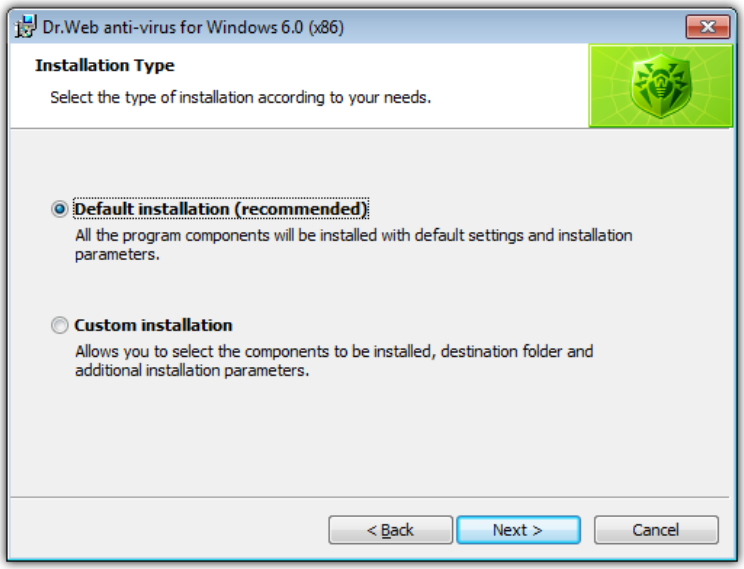
5. If in the previous step you selected the **Install Dr.Web Firewall** check box, the installation wizard will inform on possible incompatibility of **Dr.Web** with other firewalls installed on your computer and offer to uninstall or disable them. If other firewalls are installed on your computer, it is recommended to click **Cancel** and terminate installation, delete or deactivate other firewalls and after that continue installation.
   To continue installation select the **I confirm that no other firewall is installed on this computer** check box and click **Next**.
6. The installation program will bring up a warning window requesting a key file (license or demo) required for the program's operation. If a key file is present on your hard drive or on removable media, click **Browse**, select the key file and click **Next**.


Dr.Web anti-virus for Windows 6.0 (x86)
License Key File
Select the option which best suits your situation.
Dr.Web anti-virus for Windows 6.0 (x86) can only be used if you have a valid key file which regulates your rights to use the software.
Specify the path to an available valid key file
Path to key file
C:\Users\TestLab\Desktop\drweb32_x86-beta.key
Browse...
Receive key file during installation
Select this option to run the registration procedure during installation if you have a serial number or would like to receive a demonstration key file.
Receive key file later
If you select this option, Dr.Web anti-virus for Windows 6.0 (x86) will not be updated until you get a valid key file.
< Back
Next >
Cancel

If no key file is available, but you have a serial number, select **Receive key file during installation**. Otherwise, select **Receive key file later** (updating is not available in this mode) and click **Next**.

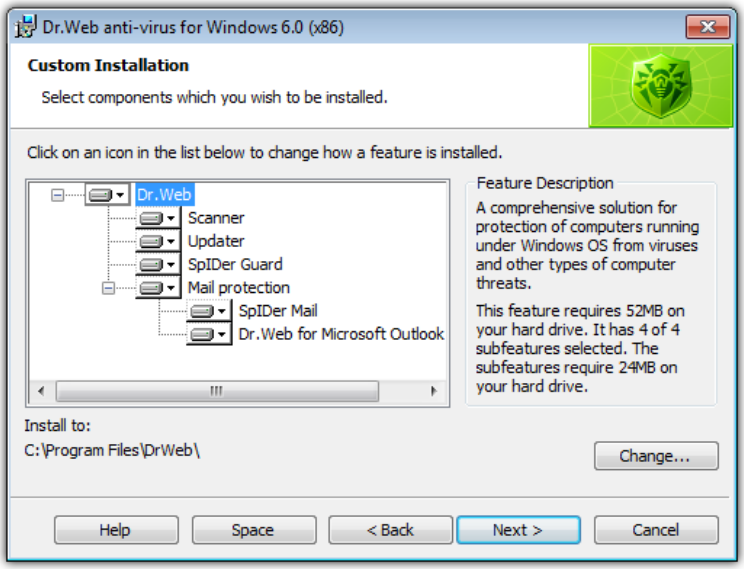
Use only **Dr.Web Anti-virus** key file. The key file should have the **.key** extension. If the key file is inside an archive, use an archiver to extract it.

7. The installation wizard will let you choose the type of installation. **Default Installation** implies installation of all components and all secondary programs automatically up to step 12. **Custom Installation** is meant for experienced users. During custom installation you will be asked to select which components should be installed, adjust proxy server settings and some additional installation parameters.


Dr.Web anti-virus for Windows 6.0 (x86)
Installation Type
Select the type of installation according to your needs.
Default installation (recommended)
All the program components will be installed with default settings and installation parameters.
Custom installation
Allows you to select the components to be installed, destination folder and additional installation parameters.
< Back
Next >
Cancel

When you choose the type of installation, click **Next**.

8. If you chose default installation type, go to step 12. In case of custom installation, a window for selecting the program components which you wish to install will open. In the hierarchical list select the components you wish to install. You can also change the installation folder if necessary.


Dr.Web anti-virus for Windows 6.0 (x86)
Custom Installation
Select components which you wish to be installed.
Click on an icon in the list below to change how a feature is installed.
Dr.Web
Scanner
Updater
SpIDer Guard
Mail protection
SpIDer Mail
Dr.Web for Microsoft Outlook
Feature Description
A comprehensive solution for protection of computers running under Windows OS from viruses and other types of computer threats.
This feature requires 52MB on your hard drive. It has 4 of 4 subfeatures selected. The subfeatures require 24MB on your hard drive.
Install to:
C:\Program Files\DrWeb\
Change...
Help
Space
< Back
Next >
Cancel

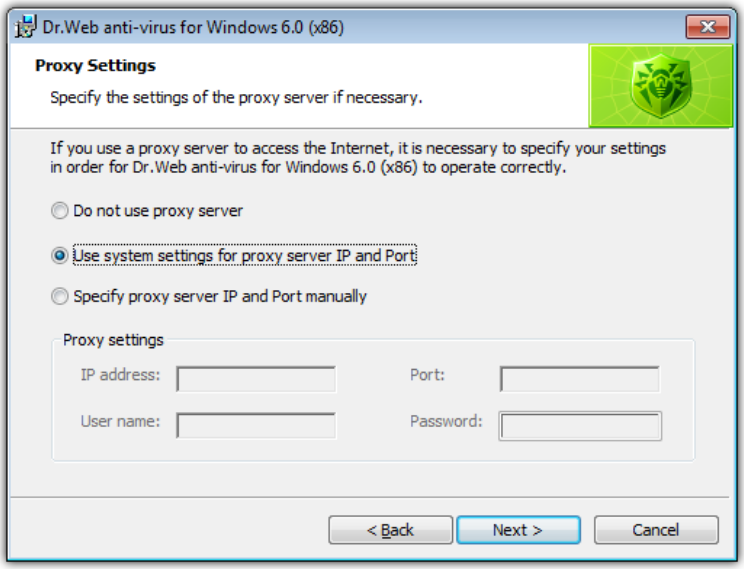
Click **Next** when you finish selecting the necessary components.

9. The window for selecting which shortcuts to **Dr.Web Anti-virus** should be created will open. Select the necessary options and click **Next**.
10. The window for adjusting proxy server settings will open.

    If you do not use a proxy server, choose **Do not use proxy server**.

    If you use current settings for proxy server, choose **Use system settings for proxy server IP and Port**.

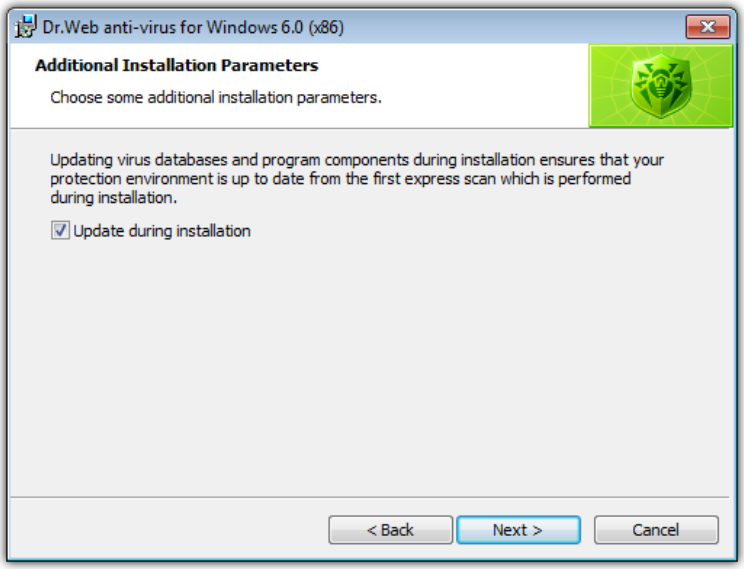
    If you want to specify settings for proxy server, choose **Specify proxy server IP and Port manually**.


Dr.Web anti-virus for Windows 6.0 (x86)
Proxy Settings
Specify the settings of the proxy server if necessary.
If you use a proxy server to access the Internet, it is necessary to specify your settings in order for Dr.Web anti-virus for Windows 6.0 (x86) to operate correctly.
Do not use proxy server
Use system settings for proxy server IP and Port
Specify proxy server IP and Port manually
Proxy settings
IP address:
Port:
User name:
Password:
< Back
Next >
Cancel

Click **Next**.

11. The window for adjusting some additional parameters of installation will open.

Select the **Update during installation** check box to download the latest virus databases during installation.


Dr.Web anti-virus for Windows 6.0 (x86)
Additional Installation Parameters
Choose some additional installation parameters.
Updating virus databases and program components during installation ensures that your protection environment is up to date from the first express scan which is performed during installation.
Update during installation
< Back
Next >
Cancel

12. A window informing that the program is ready to be installed will open. Select the **Perform full scan after installation** check box to check the file system after your computer is rebooted at the end of the installation. Then click the **Install** button to start the installation process or **Back** to change any of the installation parameters.
13. If in step 6 you selected the **Receive key file during installation** option, the **Updater** will launch the registration procedure. To receive the key file your computer should be connected to the Internet.
14. If in step 11 you selected the **Update during installation** check box, or during default installation, after receiving the key file virus databases and components of **Dr.Web Anti-virus** will be updated automatically.
15. After installation is complete the **Scanner** will perform express scan. Avert any detected threats and close the **Scanner** after the scanning process.

Scanner is not compatible with Windows Blinds (an application for adjusting Windows GUI). For correct operation of **Dr.Web Anti-virus** it is necessary to disable changing of the **Dr.Web** interface in the Windows Blinds settings. To do this, add drweb32w.exe to the list of excluded applications.

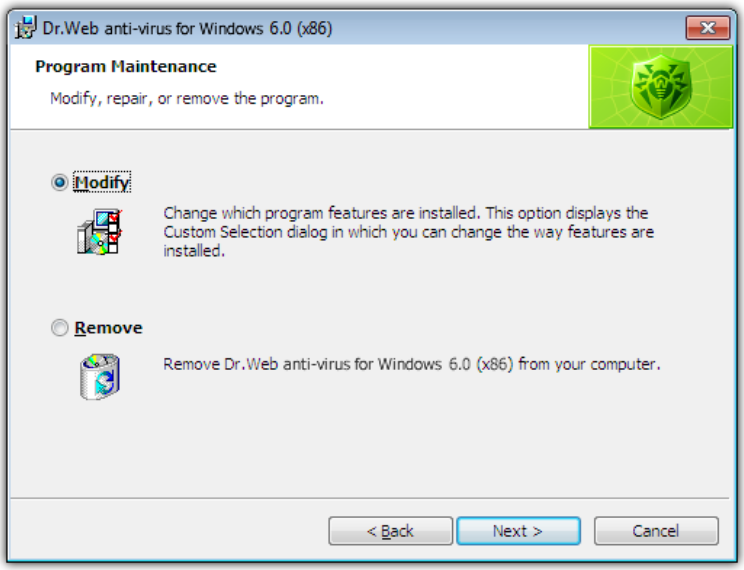
16. The program will ask for a computer reboot which is required to complete the installation.

If you install **Firewall** among other **Dr.Web Anti-virus** components under Windows Vista or Windows 7, the operating system will request the permission to install firewall drivers. For successful installation it is recommended to permit drivers installation.

Reinstalling and Removing Dr.Web Anti-virus

To modify, repair or remove an installed version of **Dr.Web Anti-virus**, start the installation wizard.

After selecting the language for the installation wizard, the following window will open:


Dr.Web anti-virus for Windows 6.0 (x86)
Program Maintenance
Modify, repair, or remove the program.
Modify
Change which program features are installed. This option displays the Custom Selection dialog in which you can change the way features are installed.
Remove
Remove Dr.Web anti-virus for Windows 6.0 (x86) from your computer.
< Back
Next >
Cancel

In this window:

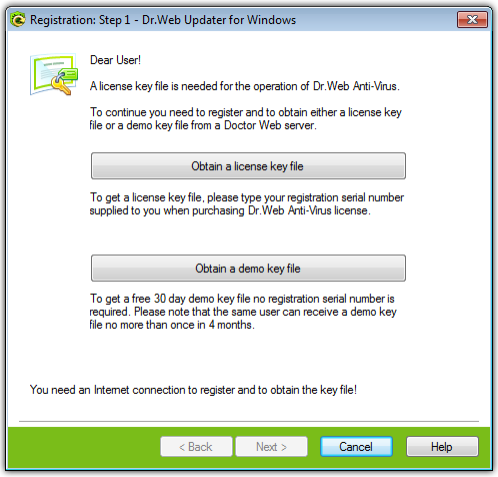
1. To change the set of installed components select **Modify** and click **Next**. The Custom Installation window will open. To remove all the components select **Remove**.
2. During removal of **Dr.Web Anti-virus** or changing the set of installed components it is necessary to disable **Self Protection**. To do this, enter the digits shown on the picture.

3. At the end of the installation, reboot the computer when prompted.

You can start the modification, repair or removal procedure via the standard Windows utility - **Add/Remove Programs**.

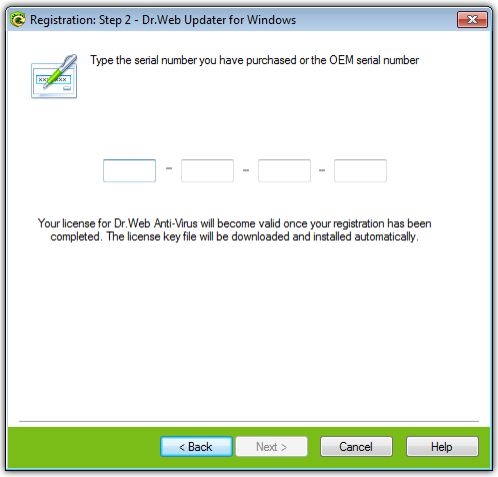
Receiving the Key File

At the first step of the procedure you will be offered to choose what type of key file you would like to obtain - either license or demo.


Registration: Step 1 - Dr.Web Updater for Windows
Dear User!
A license key file is needed for the operation of Dr.Web Anti-Virus.
To continue you need to register and to obtain either a license key file or a demo key file from a Doctor Web server.
Obtain a license key file
To get a license key file, please type your registration serial number supplied to you when purchasing Dr.Web Anti-Virus license.
Obtain a demo key file
To get a free 30 day demo key file no registration serial number is required. Please note that the same user can receive a demo key file no more than once in 4 months.
You need an Internet connection to register and to obtain the key file!
< Back
Next >
Cancel
Help

If you have a serial number, click the **Obtain a license key** file button.

In the opened window enter your serial number and click **Next**.


Registration: Step 2 - Dr.Web Updater for Windows
Type the serial number you have purchased or the OEM serial number
Your license for Dr.Web Anti-Virus will become valid once your registration has been completed. The license key file will be downloaded and installed automatically.
< Back
Next >
Cancel
Help

If you have been a user of **Dr.Web® Anti-virus For Windows** in the past, you may be eligible for extension of your new license for another 150 days. To enable the bonus, enter your registered serial number or provide the license key file. Click **Next**.

A window for entering personal data necessary to receive a key file will open. The registration procedure for receiving the demo key file starts from this step.

Fill in the fields of this window and click **Next**.

When the window with the specified information opens check that all the data is correct and click **Next**.

The procedure of receiving the license key will start. The protocol of its operation will be displayed in the information message box. If the license key is successfully downloaded, the location of the file will be indicated. Otherwise, an error message will appear.

Getting Started

The installation program allows to install the following components of **Dr.Web Anti-virus** on the computer:

- **Scanner** (GUI and console versions)
- **SpIDer Guard**
- **SpIDer Mail**
- **Dr.Web for Outlook**
- **Firewall**
- **Automatic Updating Utility**
- **SpIDer Agent**

The components of **Dr.Web Anti-virus** use common virus databases and anti-virus engine. Also uniform algorithms for detection and neutralization of viruses in scanned objects are implemented. However, the methods of selecting the objects for scanning differ greatly allowing to use these components for absolutely different and mutually supplementary PC protection policies.

For example, **Scanner for Windows** scans (on user demand or according to schedule) certain files (all files, selected logical disks, directories, etc.). By default, the main memory and startup files are scanned too. Since it is the user who decides when to launch a task, there is no need to worry about the sufficiency of computational resources needed for other important processes.

SpIDer Guard constantly resides in the main memory of the PC and intercepts calls made to the objects of the file system. The program checks for viruses files that are being launched, created or changed on the hard drives and all files that are opened on removable media and network drives. Due to a balanced approach to the level of the file system scanning details the program hardly disturbs other processes on the PC. However, this results in insignificant decrease of virus detection reliability.

An advantage of the program is uninterrupted control of the virus situation during the whole PC runtime. Besides, some viruses can only

be detected by the guard through their specific activity.

SpIDer Mail also constantly resides in the memory. The program intercepts all calls from your mail clients to mail servers via POP3/SMTP/IMAP4/NNTP protocols and scans incoming and outgoing e-mail messages before they are received (or sent) by the mail client. **SpIDer Mail** is designed to check all current mail traffic going through a computer. As a result, scanning of mailboxes becomes more efficient and less resource-consuming. For example, it allows to control attempts at mass distribution a mail worm's functional copies to the addresses specified in the user address book which is performed via the worm's own mail clients. This also allows to disable scanning of e-mail files for **SpIDer Guard**, which considerably reduces consumption of computer resources.

Dr. Web Firewall protects your computer from unauthorized access and prevents leak of vital data through networks. **Firewall** monitors connection attempts and data transfer and helps you block unwanted or suspicious connections both on network and application levels.

To secure comprehensive anti-virus protection, we advise you to use the **Dr.Web Anti-virus** components as follows:

- scan the PC's file system with the default (maximum) scanning detail settings;
- keep default settings of **SpIDer Guard**;
- perform complete e-mail scanning with **SpIDer Mail**;
- block all unknown connections with **Dr.Web Firewall**;
- perform a periodic complete scan of the PC, coordinated with the time of the virus database updates (at least once a week);
- immediately perform a complete scan in case **SpIDer Guard** was temporary disabled and the PC was connected to the Internet or files were downloaded from removable media.

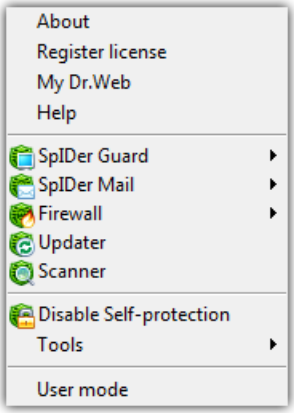
Anti-virus protection can only be effective if you update the virus databases and other files of the program regularly (preferably every hour). For more information read Automatic Updating of the Virus Databases and Other Files of the Program.

SpIDer Agent

After installing **Dr.Web Anti-virus** a **SpIDer Agent** icon is added to the taskbar notification area.

If you hover the mouse cursor over the icon, a pop-up appears with information about running components, date of last update and amount of virus signatures in the virus databases. Also, notifications which are adjusted in the settings (see below) may appear above the **SpIDer Agent** icon.

The context menu of the icon allows to perform the main management and settings functions of **Dr.Web Anti-virus**.



The **About** item opens a window with information about the version of **Dr.Web Anti-virus**.

The **Register license** item starts the registration procedure for receiving the key file from the **Doctor Web, Ltd.** server.

The **My Dr.Web** item opens your personal web page on the **Doctor Web, Ltd.** web site. This page gives information about your license

(period of usage, serial number), allows to renew your license, contact Technical Support, etc.

The **Help** item opens **Dr.Web Anti-virus** help system.

The **SpIDer Guard**, **SpIDer Mail** and **Update** items allow you to access the management and settings features of the corresponding components.

Scanner item runs **Dr.Web Scanner**.

The **Disable/Enable Self-protection** item allows to disable/enable protection of **Dr.Web Anti-virus** files, registry keys and processes from damage and deletion.

To disable self-protection:

- select **Disable self-protection** in the **SpIDer Agent** menu;
- enter text displayed on the picture.

The **Enable self-protection** item will appear.

You cannot disable self-protection in User mode. It is not recommended to disable self-protection.

If any problems occur during operation of defragmentation programs, disable self-protection temporary.

The **Tools** item opens a submenu which contains following items:

- **License Manager** (see License Manager).
- **Settings**. This command displays SpIDer Agent settings.
- **Scheduler.** This command displays the standard Windows Scheduler task which determines the **Dr.Web® Anti-virus For Windows** updating schedule.
- **Quarantine** (see Quarantine);
- to report generation.

Before contacting **Doctor Web technical support**, generate the report on your OS and **Dr.Web** operation. For parameters adjustment, in the opened window click **Report settings**. The report will be stored as an archive in the DoctorWeb subfolder of

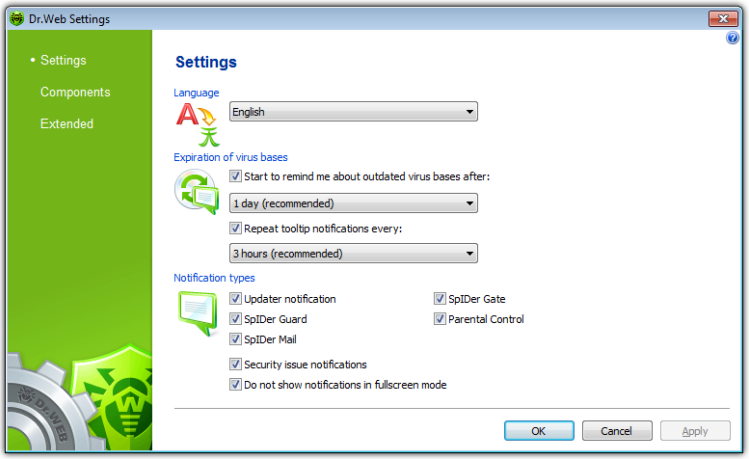
the %USERPROFILE% directory.

The **Administrative**/**User mode** item allows you to switch between full-function **Administrative mode** and restricted **User mode**. In **User mode**, access to settings of components and **Updater** is forbidden, and the **Scheduler** item is also inaccessible as well as disabling of **SpIDer Guard**, **Dr.Web Firewall** or self-protection. You need administrative rights to switch to **Administrative mode**.

This item displays when you do not have administrative privileges. For instance, this item displays when you log into Microsoft Windows 2000 or Windows XP operating systems as a non-privileged user, or when User Account Control of Windows Vista or Microsoft Windows 7 operating system is enabled. Otherwise, the item is hidden and **Dr.Web Anti-virus** operates in full-function mode all the time.

SpIDer Agent Settings

Settings Page



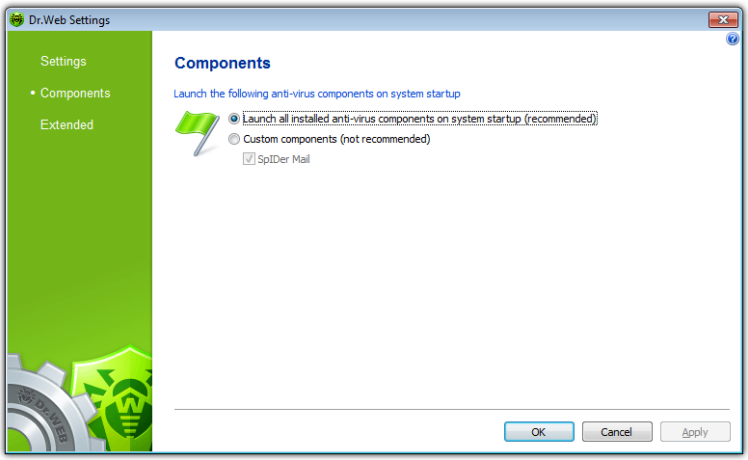
On the **Dr.Web Settings** page you can specify the language of the **Dr.Web Anti-virus** GUI by selecting the necessary language in the **Language** list. If you choose language that hasn't been installed, **Dr. Web** will suggest to install it.

Also in this window you can select the types of pop-up notifications which appear above the **SpIDer Agent** icon in the taskbar notification area. Components send notifications when a corresponding event happens (i.e. when a threat is detected or an update is performed). Also if your system hasn't been scanned for 7 days, a corresponding notification appears (**Security issue notifications** checkbox).

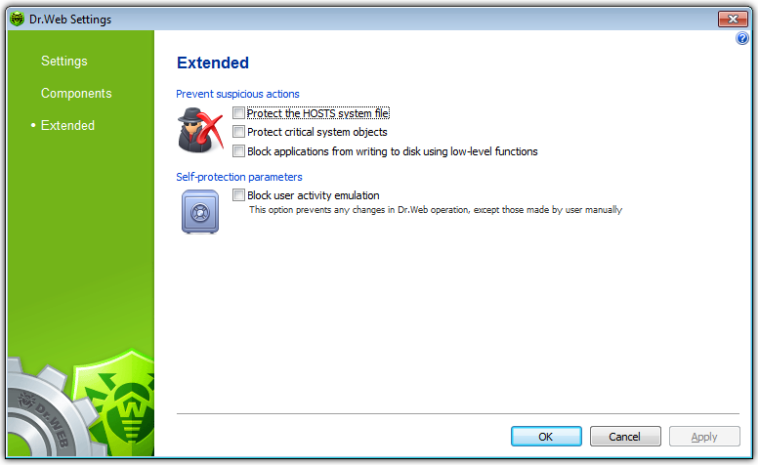
Components page

On the **Components** page you can choose one of the following:

- **Launch all installed anti-virus components on system startup (recommended)**.
- **Custom components (not recommended)**. In this mode you can disable automatic launch of some components.



Extended page

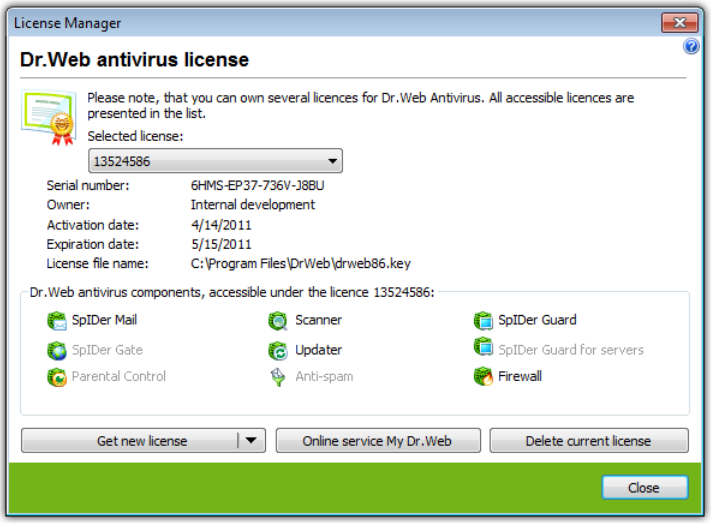


On this page, you can specify self-protection parameters and disable miscellaneous operations that may compromise security of your computer.

If any problems occur during installation of important Microsoft updates or installation and operation of programs (including defragmentation programs), disable the corresponding options in this group.

License Manager

License Manager shows information from the **Dr.Web Anti-virus** key files in an understandable form.



Selected **Dr.Web Anti-virus** components for your license are specified in the **Dr. Web antivirus components** group box.

The **Online service My Dr.Web** item opens your personal web page on the official **Doctor Web** web site. This page gives information about your license (period of usage, serial number), allows to renew your license, contact Technical Support, etc.

To start the registration procedure for receiving the key file from the **Doctor Web** server, click the **Get new licence** button and choose **from Internet** in the drop-down menu. That will launch receiving the key file procedure.

To add a key file

1. Press the **Get new licence** button. Choose **from file** in the drop-down menu.
2. Select the file in a standard window.
3. **Dr.Web Anti-virus** will automatically start to use a key file.

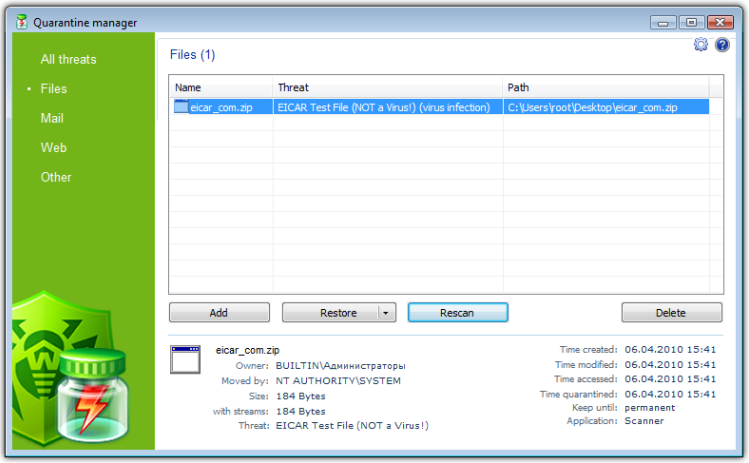
If you received a key file during installation or in the distribution kit complete set, installation of a key file is made automatically and does not demand any additional actions.

To delete a key file from a list, select it and click the **Delete current licence** button. Last used key cannot be removed.

Quarantine

Special **Quarantine** section of **Dr.Web Anti-virus** serves for isolation of files that are suspicious as malware. The **Quarantine** folder is created separately on each logic disk where suspicious files have been found. When infected objects are detected at the portable data carrier accessible for writing, the Quarantine folder will be created on the data carrier and infected objects will be moved to this folder.

To view and edit the quarantine, select **Quarantine** in the **Tools** submenu of the **SpIDer Agent** context menu. A new window with table that contains quarantine current state opens.



In the center of the window the table with the quarantine state is displayed. The following columns are included:

- **Name** – name list of the objects in the quarantine,
- **Threat** – malware classification, which is assigned by **Dr.Web Anti-virus** during automatic moving to the quarantine.
- **Path** – full path of the object before moving to the quarantine.

The bottom pane of the window displays detailed information about the selected objects. You can also display this information in the table.

To configure table view

1. Right-click the header of the table and select **Customize columns**.
2. In the opened window, set the checkboxes next to those items that you want to display in the table, or clear the checkboxes next to those items that you want to hide. You can also do one of the following:
   - To select checkboxes for all items, click **Check all**.
   - To clear all checkboxes, click **Uncheck all**.
3. Use **Move up** and **Move down** to change position of a column in the table.
4. After editing, click **OK** to save the changes or **Cancel** to cancel them.

The left pane serves to filter the quarantine objects to display. Click the corresponding option to display all quarantine objects or just specified groups: files, mail objects, web pages or all other objects, not classified.

In the quarantine window only the users with access rights to the files can see these that files.

Use the following buttons to manage the quarantine:

- **Add** – add the file to the quarantine. Select the necessary file in the opened file system browser.
- **Restore** – remove the file from the quarantine and restore the original location of the file, i.e. restore the file to the folder where it had resided before it was moved to the quarantine.

Use this option only when you are sure that the objects are not harmful.

In the drop-down menu you can choose **Restore to** – restore the file to the folder specified by the user.

- **Rescan** – scan the file one more time.
- **Remove** – delete the file from the quarantine and from the system.
- **Submit file(s) to Doctor Web Laboratory** – send file to **Doctor Web Virus Laboratory** for checking.

To manage several objects simultaneously, select necessary objects in the quarantine window and select necessary action in the drop-down menu.

In the bottom of the quarantine window the detailed information about selected items is displayed.

To configure **Quarantine** parameters, click the button in the **Quarantine** window. The **Quarantine** properties window will be opened. In this window you can change the following parameters:

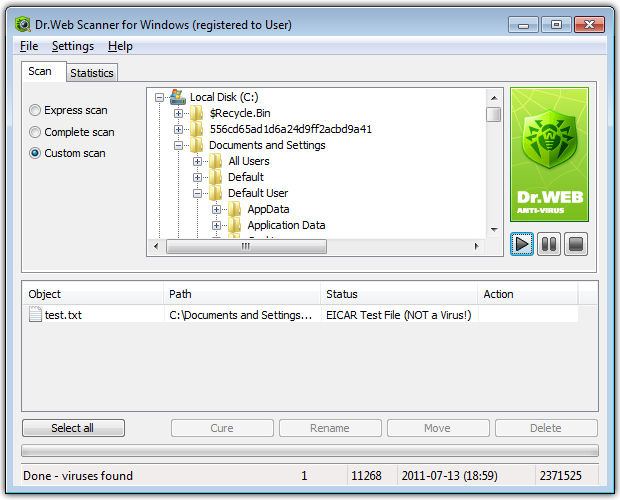
- In the **Set quarantine size** section you can configure the amount of disk space for **Quarantine** folder.
- In the **View** section, you can set the **Show backup files** flag to display backup copies of **Quarantine** files in the object's table.

Backup copies are created automatically during moving files to the **Quarantine**. Even if **Quarantine** files are kept permanently, their backup copies are kept temporarily.

Using Dr.Web Scanner for Windows

By default, the program scans all files for viruses using both the virus database and the heuristic analyzer (a method based on the general algorithms of virus developing allowing to detect the viruses unknown to the program with a high probability). Executable files compressed with special packers are unpacked when scanned. Files in archives of all commonly used types (ACE, ALZIP, AR, ARJ, BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP), in containers (1C, CHM, MSI, RTF, ISO, CPIO, DEB, RPM), and in mailboxes of mail programs (the format of mail messages should conform to RFC822) are also checked.

By default, **Dr.Web Anti-virus** informs a user about any infected or suspicious objects in a special report field generated at the bottom of the **Scanner** main window (see illustration below). For more information see Adjusting the Scanner Settings.



Launching Scanner. General Information.

If your system hasn't been scanned for 7 days, a corresponding notification appears (see SpIDer Agent).

Scanner is installed as a usual Windows application and can be launched by the user or automatically (see Automatic Launch of Tasks for Scanning and Updating in Dr.Web).

It is recommended for the scanner to be run by a user with administrator rights because files to which unprivileged users have no access (including system folders) are not scanned.

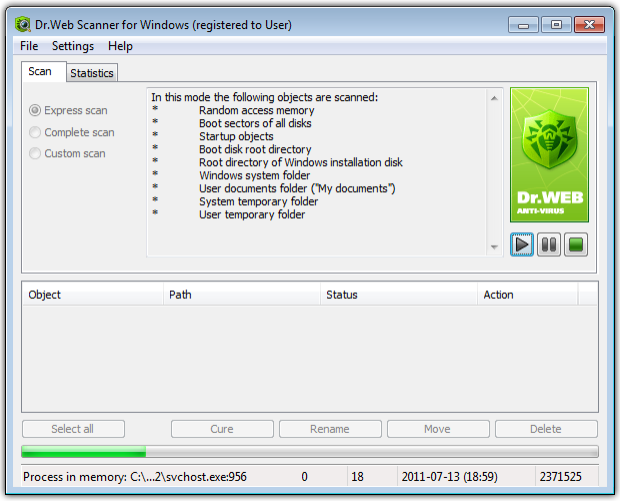
To launch the Scanner do one of the following:

- Click the **Dr. Web Scanner** icon on the Desktop.
- Click the **Scanner** item in the context menu of the **SpIDer Agent** icon in the taskbar notification area (see SpIDer Agent chapter).
- Click the **Dr.Web Scanner** item in All Programs -> Dr.Web directory of the Windows **Start** menu.
- Run the corresponding command in the Windows command line (read Command Line Scanning Mode).

You can also run **Scanner** with default settings to scan a certain file or folder immediately:

- Select **Check by Dr.Web** in the context menu of the file or folder icon (on the Desktop or in Windows Explorer).
- Drag and drop the icon of the file or folder onto the **Scanner** icon or to the main window of **Scanner** (see illustration below).

When **Scanner** launches its main window opens.


Dr.Web Scanner for Windows (registered to User)
File Settings Help
Scan Statistics
Express scan
Complete scan
Custom scan
In this mode the following objects are scanned:
* Random access memory
* Boot sectors of all disks
* Startup objects
* Boot disk root directory
* Root directory of Windows installation disk
* Windows system folder
* User documents folder ("My documents")
* System temporary folder
* User temporary folder
Dr.WEB
ANTI-VIRUS
Object Path Status Action
Select all Cure Rename Move Delete
Process in memory: C:\...2\svchost.exe:956 0 18 2011-07-13 (18:59) 2371525

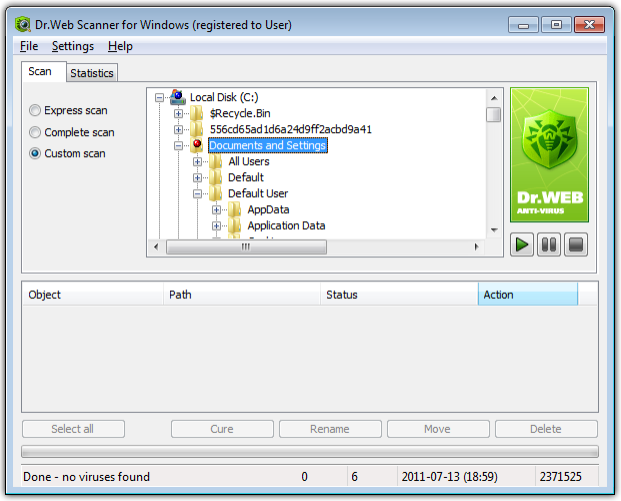
There are 3 scanning modes: **Express scan**, **Complete scan** and **Custom scan**. Depending on the selected mode, either a list of objects which will be scanned or a file system tree is displayed at the center of the window.

In **Express scan** mode the following objects are scanned:

- Random access memory
- Boot sectors of all disks
- Autorun objects
- Boot disk root directory
- Windows installation disk root directory
- Windows system folder
- User documents folder ("My documents")
- System temporary folder
- User temporary folder

If **Complete scan** mode is selected, random access memory, all hard drives and removable media (including boot sectors of all disks) are scanned.

Custom scan mode allows you to select folders and files for scanning. When this mode is selected, a file system tree will appear in the center of the **Scan** pane. If necessary, you can expand objects in the file system tree down to the level of any folder or file. Select the necessary objects for scanning in the file system tree. The illustration below shows the situation when the Documents and Settings folder on the C logical disk is selected for scanning.



To launch scanning of the selected objects, click the button in the right part of the main window.

When launching **Scanner** on a portable computer running on battery, a message on the battery state will appear. You can disable this option in the **General** tab of the **Settings** window (for more information see Adjusting the Scanner Settings).

As soon as scanning starts, the button in the right part of the window becomes available. Click this button to pause the scanning process. To resume scanning, click the button. To stop scanning, click the button.

By default, subfolders in the selected directories and logical drives, as well as boot sectors of all logical drives on which at least one folder or file is selected, and also the main boot sectors of respective physical drives are scanned too.

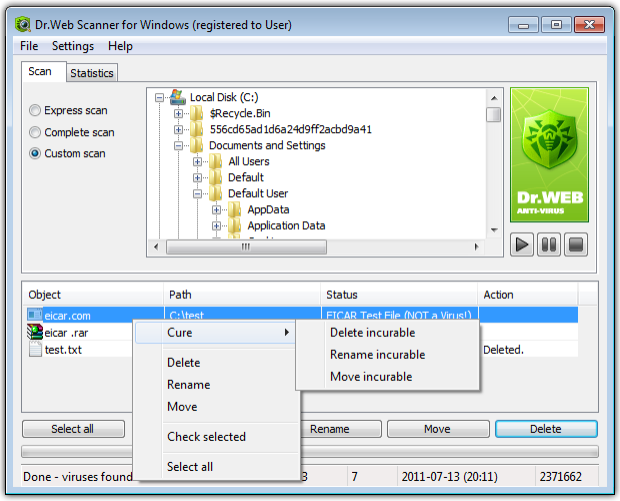
If express or complete scanning mode is set, **Scanner** will define, whether the HOSTS-file (the text file which contains a database of domain names and is used at their translation in network addresses) has been changed. The HOSTS-file can be changed by malicious software (for example, on purpose to redirect the user on a certain web site). In case the HOSTS-file has been changed, **Scanner** will suggest to restore its initial condition. It will allow to eliminate unapproved change of the file by malicious software.

Actions Upon Detection of a Virus

By default, if a known virus or a suspicious object is detected, **Scanner** informs you about it in the report field located at the bottom of the **Scan** tab. Infected processed in computer memory are terminated automatically. Trojan programs are deleted upon detection.

To apply actions to detected objects

1. Right click the line of the report list with the description of the infected object.



You can specify an action either for all objects or for specific objects in the report list. To select all objects click the **Select All** button. To select objects in the report list the following keys and combinations of keys are additionally used:

- [Insert] - to select an object.
- [CTRL+A] - to select all objects.
- the asterisk button [*] on numeric keyboard - to select or deselect all.

2. Select the action you want to apply in the opened context menu or click the corresponding button at the bottom of the report field.

3. If the **Cure** action is selected, choose another action which should be applied in case curing fails.

The **Rename** action means replacement of a file extension. By default, the first character of the extension is replaced with the # symbol.

The **Move** action means that the object is moved to a folder specified in the program's settings. By default, it is the infected.!!! subfolder of the program's installation directory.

The **Delete** action means that the infected object is deleted.

Suspicious objects are moved to infected.!!! folder and should be sent for analysis to the anti-virus laboratory of **Doctor Web, Ltd.** through a specially designed web-form at http://support.drweb.com/sendnew/.

For suspicious objects curing is impossible.

For objects which are not files (boot sectors) moving, renaming and

deletion is impossible.

For files inside archives, containers or attachments, no actions are possible.

By default, when the **Delete** action is applied to file archives, containers or mailboxes, the program generates a warning message that the data might be lost.

After the required action is applied, the report with the operation result will be generated in the **Action** column of the report field.

In some cases the specified action cannot be immediately applied to selected files. The **Will be cured after reboot** or **Will be deleted after reboot** text string, depending on the action specified, will appear in the **Action** column of the **Scanner** main window report field. The necessary action will be taken at the next reboot, i.e. it will be a postponed action. That is why, if such objects are found, it is recommended to reboot the system immediately after the scanning process. You can also set up automatic reboot if necessary (for more information see Adjusting the Scanner Settings).

The detailed report on the program's operation is saved as a log file. By default, the log file resides in the program's installation folder in the DoctorWeb subfolder of the %USERPROFILE% directory. The name of the log file is drweb32w.log.

Adjusting Scanner Settings

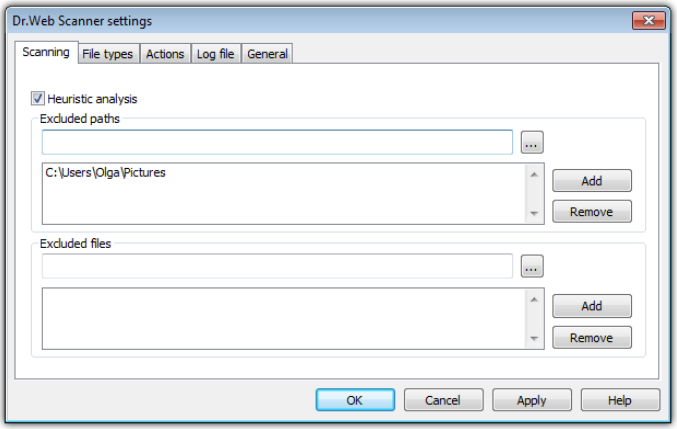
It is recommended for **Scanner** to be run by a user with administrator privileges because files to which unprivileged users have no access (including system folders) are not scanned.

Default program settings are optimal for most applications and they should not be modified, if there is no special need for it.

To modify the Scanner settings:

1. To open **Scanner** settings do one of the following:
   - Select the **Options** item in the menu located at the top of the main window and then choose **Change settings** in the opened submenu.
   - Make sure, that **Scanner** window is active, and press F9.

   This will open the **Scanner settings** window which contains several tabs.



2. Make the necessary changes and click **Apply** when switching to another pane.

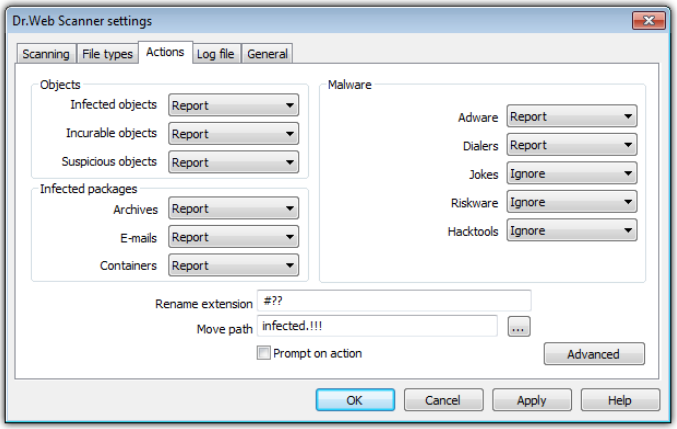
3. For more detailed information on the settings specified in each tab use the **Help** button. Also, for the majority of settings specified in the panes, a context help feature is available which is activated by right-clicking an element of the interface.
4. When editing is finished click **OK** to save the changes made or **Cancel** to cancel the changes.

The most frequent changes in default settings are described below.

The default settings of **Dr.Web Anti-virus** are optimal for scanning on user demand. The program performs full and detailed scanning of the selected objects and informs the user on all infected or suspicious objects, leaving him with the right to decide what action should be taken upon their detection. The objects containing joke programs, riskware or hacktools are excluded: for them the **Ignore** action is specified by default. However, when scanning is performed without the user's assistance, settings for automatic reaction of the program upon detection of infected objects can be applied.

To set the program's reaction upon detection of infected objects:

1. Select the **Actions** tab in the **Scanner settings** window.



2. In the **Infected objects** drop-down list, select the program's action upon detection of an infected object.

The **Cure** action is the best for automatic mode.

3. Select the program's action upon detection of an incurable object in the **Incurable objects** drop-down list. The range of actions is the same as those described above but the **Cure** action is not available.

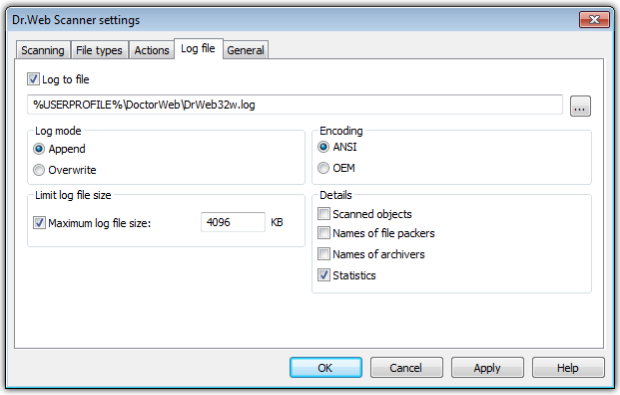
The **Move to** action is the best in most cases.

4. In the **Suspicious objects** drop-down list select the program's action upon detection of a suspicious object (fully similar to the previous paragraph).

It is recommended to keep the default **Report** action.

5. Similar actions should be specified for detection of objects containing Adware, Dialers, Jokes, Riskware and Hacktools.
6. The same way the automatic actions of the program upon detection of viruses or suspicious codes in file archives, containers and mailboxes, applied to these objects as a whole, are set up. The **Report** action is specified by default.
7. Clear the **Prompt on action** check box to enable the specified program's action without prior inquiry.
8. When **Rename** is set as the program's action, the program, by default, will replace the first character of a file name extension with the **#** symbol. If necessary, you can change the renaming mask for file extensions. For this, insert the necessary value into the **Rename extension** entry field.
9. When **Move to** is set as the program's action, the program, by default, will move the file to the infected.!!! subfolder of the program's installation directory. If necessary, you can specify a different name of the folder in the **Move path** entry field.
10. To cure some infected files it is necessary to reboot Windows. You can adjust parameters of rebooting in the **Cure settings** window. To open this window click the **Advanced** button in the bottom right of the **Actions** pane. You can choose one of the following:
    - **Restart automatically, if necessary**. It can lead to loss of unsaved data.
    - **Do not restart automatically**. If you choose this mode, it is recommended to select the **Prompt restart, when necessary** checkbox to restart at any time convenient to you.

In the **Log file** tab you can set up the parameters of the log file.



Most parameters set by default should be left unchanged. However, you can change the details of logging (by default, the information on infected or suspicious objects is always logged; the information on the scanned packed files and archives and on successful scanning of other files is omitted). You can instruct to log the results of scanning of all files, regardless the result. For this, select the **Scanned objects** check box (this will considerably increase the size of the log file). You can instruct to log the names of archivers (select the **Archivers names** check box) and executable file packers (select the **File packers names** check box).

You can cancel the default restriction set for the maximum size of the log file (clear the **Maximum log file size** check box) or specify your own log file size limit in the entry field next to the check box.

Command Line Scanning Mode

You can run **Dr.Web Scanner for Windows** in the command line mode which allows to specify settings of the current scanning session and the list of objects for scanning as additional parameters. This mode provides automatic activation of **Scanner** according to schedule.

The launching command syntax is as follows:

[*path_to_program*] `drweb32w` [*objects*] [*keys*]

The list of objects for scanning can be empty or contain several elements separated with blanks.

The most commonly used examples of specifying the objects for scanning are given below:

- ***** – scan all hard drives
- **C:** – scan drive C:
- **D:\games** – scan files in the specified folder
- **C:\games*** – scan all files and subfolders of the specified directory

Switches are command line parameters which specify the program's settings. If no switches are defined, scanning is performed with the settings specified earlier (or with the default settings if you have not changed them).

Each switch begins with a forward slash (**/**) character and is separated with a blank from other switches.

Several most frequently used switches are listed below. For their full list refer to Appendix A.

/cu – cure infected objects.

/icm – move incurable files (to the default folder).

/icr – rename (by default).

/qu – close the scanner window after session is finished.

/go – no prompts on actions should be generated.

Two last parameters are especially useful for automatic launch of **Scanner** according to schedule.

DrWebWcl Console Scanner can be used with the same parameters. To do this, type the **drwebwcl** command name instead of **drweb32w**.

By default, the console version of **Scanner for Windows** uses the same settings as the GUI-version of **Scanner**. The parameters set via the graphical interface of **Scanner** (for more information see Adjusting the Scanner Settings) are used for scanning in command line mode unless different parameters were set as switches. Some settings of **Scanner** can only be specified in the program's configuration file (read Appendix B for more details).

DWScancl Console Scanner

Dr.Web Anti-virus also includes **DWScancl Console Scanner**. In contrast to **DrWebWcl Console Scanner**, **DWScancl Console Scanner** is designed for multiprocessors and provides advanced settings (larger amout of switches).

DWScancl Console Scanner moves suspicious files not to the infected.!!! folder, but to **Quarantine**.

The launching command syntax is as follows:

[*path_to_program*] `dwscancl` [*keys*] [*objects*]

The list of objects for scanning can be empty or contain several elements separated with blanks.

Parameter starts with **/** symbol, several parameters are divided by spaces. All parameters are listed in Appendix A.

Return codes:

0 – scanning was completed successfully, infected objects were not found

1 – scanning was completed successfully, infected objects were detected

10 – invalid keys are specified

11 – key file is not found or does not support **DWScancl Console Scanner**

12 – Scanning Engine did not start

255 – scanning was aborted by user request

SpIDer Guard for Windows

By default, **SpIDer Guard** is loaded automatically at every Windows startup and cannot be unloaded during the current Windows session. If it is necessary to temporarily disable **SpIDer Guard** (for example, when a task consuming too much processor resources is performed in real time mode), select the **Disable** item in the menu of **SpIDer Guard** item (read SpIDer Agent).

Only the user with administrator rights can temporarily disable **SpIDer Guard**.

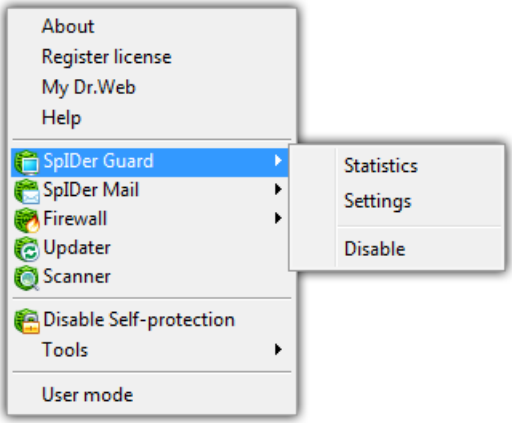
By default, **SpIDer Guard** performs on-access scanning of files that are being created or changed on the HDD and all files that are opened on removable media. It scans these files in the same way as the **Scanner** but with "milder" options. Besides, **SpIDer Guard** constantly monitors running processes for virus-like activity and, if they are detected, blocks these processes.

By default, upon detection of infected objects **SpIDer Guard** supplied with **Dr.Web Anti-virus** acts according to actions set on Actions tab.

You can set the program's reaction to virus events by adjusting the corresponding settings. A user can control it with the help of the **Statistics** window and the log file.

Managing the Guard

Main tools for setting and managing in **SpIDer Guard** reside in its menu.



The **Statistics** menu item allows to open the **Statistics** window, where the information on the operation of **SpIDer Guard** during the current session is displayed (the number of scanned, infected or suspicious objects, virus-like activities and actions taken).

The **Settings** menu item gives access to the main part of the program parameters (for details, see Main Parameters of SpIDer Guard).

The **Disable** item allows to temporary disable program functions (for users with administrator rights only).

Access to the **SpIDer Guard** settings is possible only for the user with administrator rights.

To disable **SpIDer Guard**, enter confirmation code.

Main Parameters of the SpIDer Guard

The main adjustable parameters of **SpIDer Guard** are in the **Settings** panel. To receive help on parameters specified on a page, select that page and click **Help** .

When you finish editing the parameters click **OK** to save changes or **Cancel** to cancel the changes made.

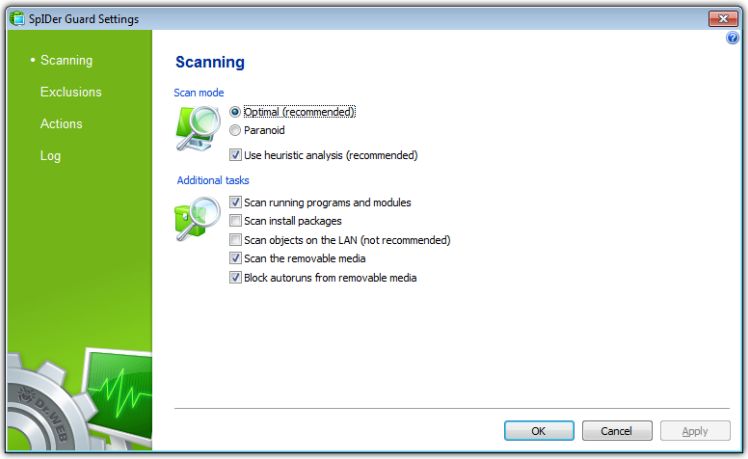
Some of the most frequently changed settings of the program are described below.

Scanning Page

By default, **SpIDer Guard** is set in **Optimal** mode to scan files that are being executed, created or changed on the hard drives and all files that are opened on removable media.

In **Paranoid** mode **SpIDer Guard** scans files that are being opened, created or changed on the hard drives, on removable media and network drives.

Selecting the **Use heuristic analysis** checkbox enables the heuristic analyser mode (a method of virus detection based on the analysis of actions specific for viruses).



Certain external devices (e.g. mobile drives with USB interface) can be identified by the system as hard drives. That is why such devices should be used with utmost care and checked for viruses by the **Scanner** when connected to a computer.

Disabled scanning of archives, even if **SpIDer Guard** is constantly active, means that viruses can still easily penetrate a PC but their detection will be postponed. When the infected archive is unpacked (or an infected message is opened), an attempt to write the infected object on the hard drive will be taken and **SpIDer Guard** will inevitably detect it.

In **Additional tasks** group, you can configure **SpIDer Guard** parameters to check the following objects:

- Executables of running processes regardless of their location
- Installation files
- Files on network drives
- Files and boot sectors on removable devices

These parameters are applied in any scan mode.

Also you can select **Block autoruns from removable media** check-

box to disable autoplay option for portable data storages such as CD/DVD, flash memory etc. This option helps to protect you computer from viruses transmitted via removable media.

If any problem occur during installation with autorun option, it is recommended to remove **Block autoruns from removable media** flag.

Exclusions Page

On this page folders and files to be excluded from checking are specified.

In the **Exluded folders and files** field the list of folders and files to be excluded from scanning can be set. These can be the quarantine folder of the anti-virus, some program folders, temporary files (swap files), etc.

To add a file, folder or mask to the list type its name into the entry field and click **Add**. To enter an existing file name or folder you can click the **Browse** button to the right and select the object in a standard file browsing window.

To remove a file or folder from the list select it in the list and click **Remove**.

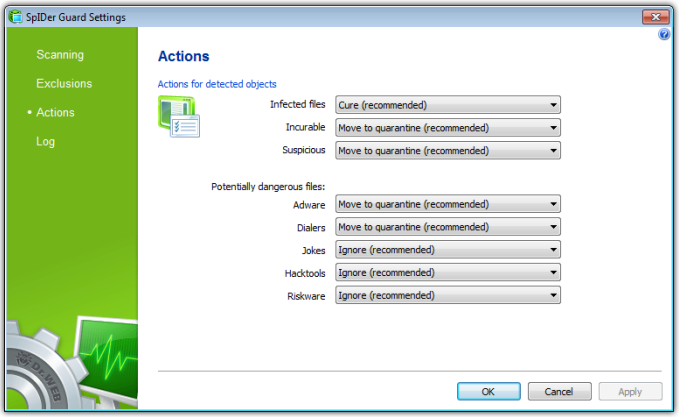
Actions Page

On this page you can adjust **SpIDer Guard** reaction to infected objects.

The **Cure**, **Ignore**, **Delete** and **Move to quarantine** actions are similar to those of the **Scanner**.

To change the default actions in SpIDer Guard:

1. In the **SpIDer Guard Settings** window select the **Actions** tab.



2. In the **Infected objects** drop-down list choose the program's action upon detection of an infected object. **Cure** action is recommended.
3. In the **Incurable objects** drop-down list choose the program's action upon detection of an incurable object. **Move to quarantine** action is recommended. Other actions with moved files are described in Actions Upon Detection of a Virus chapter.
4. In the **Suspicious objects** drop-down list choose the program's action upon detection of a suspicious object. **Move to quarantine** action is recommended.
5. In the **Adware** and **Dialers** drop-down lists choose the program's action upon detection of dangerous files. **Move to quarantine** action is recommended.
6. The same procedure is used when setting the program's actions upon detection of objects containing jokes, riskware and hacktools. **Ignore** action is recommended.
7. Click **OK** to apply changes and close the **SpIDer Guard Settings** window.

Log Page

On this page, you can select the mode of keeping records in the log file:

- **Standard** – in this mode, **SpIDer Guard** logs the following most important actions only:
  - Time of updates
  - Time of **SpIDer Guard** starts and stops
  - Detected errors and infections
- **Extended** – in this mode, **SpIDer Guard** logs the most important actions and the following additional data:
  - Names of scanned objects
  - Names of packers
  - Contents of scanned complex objects (archives, mail boxes and file containers)

  It is recommended to use this mode when determining objects that **SpIDer Guard** checks most often.
- **Debugging** – in this mode, **SpIDer Guard** logs all details on its activity. This may result in considerable log growth.

SpIDer Mail

By default, **SpIDer Mail for Windows** is included into the set of installed components, constantly resides in the memory and automatically reloads at Windows startup. You can disable the automatic launch mode in SpIDer Agent settings.

By default, the program automatically intercepts all calls of any mail programs on your computer to POP3 servers on port 110, to SMTP servers on port 25, to IMAP4 servers on port 143 and to NNTP servers on port 119.

Any incoming messages are intercepted by **SpIDer Mail** before they are received by the mail client. They are scanned for viruses with the maximum possible level of detail. If no viruses or suspicious objects are found they are passed on to the mail program in a "transparent" mode, as if it was received immediately from the server. Similar procedure is applied for outgoing messages before they are sent to servers.

By default, the program's reaction upon detection of infected incoming messages, as well as messages that were not scanned (e.g. due to their complicated structure) is as follows:

- Messages infected with a virus are not delivered; the mail program receives an instructions to delete this message; the server receives a notification that the message had been received (this action is called *deletion* of the message).
- Messages with suspicious objects are moved to the quarantine folder as separate files; the mail program receives a notification about this (this action is called *moving* the message).
- Messages that were not scanned and safe messages are passed on.
- All deleted or moved messages are also deleted from the POP3 or IMAP4 server.

Infected or suspicious outgoing messages are not sent to the server; a user is notified that a message will not be sent (usually the mail program will save it).

If an unknown virus distributing through e-mail is detected on the computer, the program can detect signs of a typical "behavior" for such viruses (mass distribution). By default, this option is enabled.

The default program settings are optimal for a beginner, provide maximum protection level and require minimum user interference. But some options of mail programs are blocked (for example, sending a message to many addresses might be considered as mass distribution and mail will not be scanned for spam), useful information (from their safe text part) becomes unavailable if messages are automatically destroyed. Advanced users can modify mail scanning parameters and the program's reactions to virus events.

In certain cases automatic interception of POP3, SMTP, IMAP4 and NNTP connections is impossible; in such situation the program allows to set up manual interception of connections.

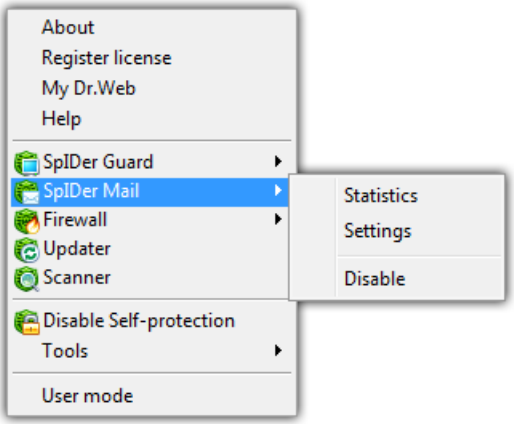
Dr.Web Scanner can also detect viruses in mailboxes of several formats, but **SpIDer Mail** has several advantages:

- Not all formats of popular mailboxes are supported by **Dr.Web Scanner**. In this case, when using **SpIDer Mail**, the infected messages are not even delivered to mailboxes.
- The **Scanner** does not check the mailboxes at the moment of the mail receipt, but either on user demand or according to schedule. Furthermore, this action is rather resource-consuming and takes a lot of time.

Thus, with all the components in their default settings, **SpIDer Mail** detects viruses and suspicious objects distributed via e-mail first and does not let them infiltrate into your computer. Its operation is rather resource-sparing; scanning of e-mail files can be performed without other components.

Managing SpIDer Mail

SpIDer Mail can be managed via the **SpIDer Mail** item in the context menu of the **SpIDer Agent** icon (see SpIDer Agent).



If the **Settings** menu item is selected, a window with **SpIDer Mail** settings will open (read Adjusting Certain Program Settings).

User should have administrator rights to change settings of the **SpIDer Mail** interface.

If the **Statistics** menu item is selected, a window with information on the program's operation during current session (the number of scanned, infected, suspicious objects and taken actions) will open.

The **Disable**/**Enable** item allows to start/stop **SpIDer Mail**.

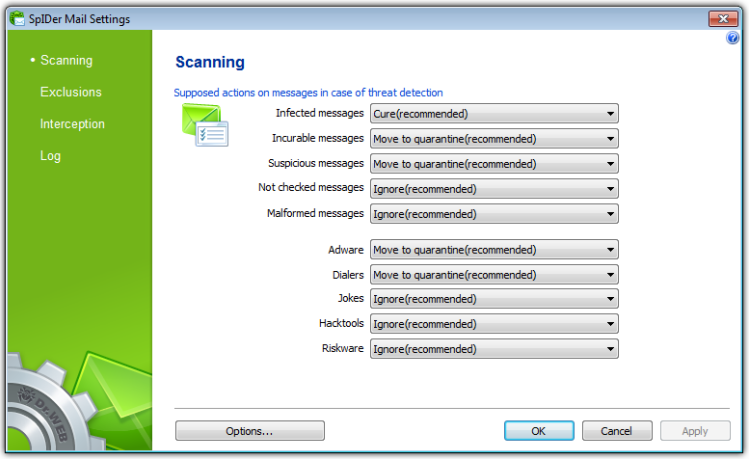
Adjusting Certain Program Settings

To modify **SpIDer Mail** settings open the settings window as described in Managing SpIDer Mail.

When editing the settings, use the program's help system (general help for each page is generated by pressing the Help button; there is also a context prompt for certain elements of the interface).

When adjusting is finished, click **OK**.

Most default settings are optimal for the majority of situations. The most frequently used parameters, except the default ones are described below.



To change the default actions in SpIDer Mail:

1. In the **Infected messages** drop-down list choose the program's action upon detection of an infected message (**Cure** action is recommended).
2. In the **Incurable messages** drop-down list choose the program's action upon detection of an incurable

message (**Move to quarantine** action is recommended). Other actions with moved files are described in Actions Upon Detection of a Virus.

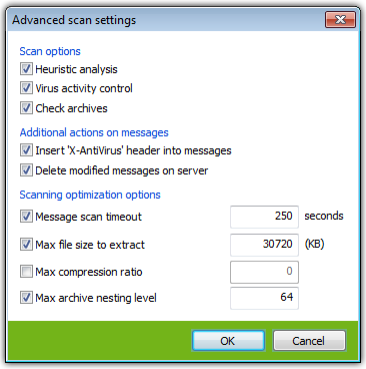
3. In the **Suspicious messages** drop-down list choose the program's action upon detection of a suspicious message. (**Move to quarantine** action is recommended).
4. In the **Non checked messages** and **Malformed messages** drop-down lists choose the program's action upon detection of a non-checked or malformed message. (**Ignore** action is recommended).
5. In the **Adware** and **Dialers** drop-down lists choose the program's action upon detection of adware and dilers. (**Move to quarantine** action is recommended).
6. The same procedure is used when setting the program's actions upon detection of messages containing jokes, riskware and hacktools. (**Ignore** action is recommended).
7. Click **OK** to apply changes and close the **SpIDer Mail Settings** window.

Protection against suspicious messages can be disabled if a PC is additionally protected by a constantly loaded **SpIDer Guard** component.

Additionally, you can increase the default level of reliability of anti-virus protection by selecting the **Move to quarantine** option in the **Not checked messages** drop-down list. Files with moved messages should be checked by the scanner.

Experienced users can disable the mode when the deleted or moved messages are immediately deleted from the POP3/IMAP4 server, and delete such messages manually or using more advanced settings of the mail program. For this, clear the **Delete modified messages on server** check box in advanced settings.

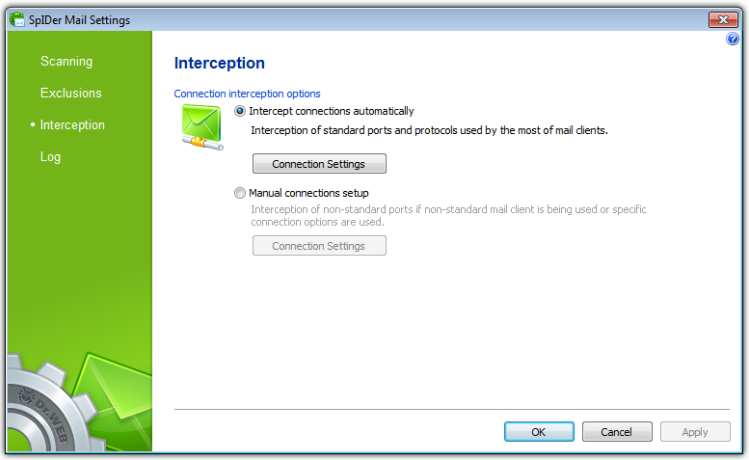
To get access to advanced settings click the **Options** button.



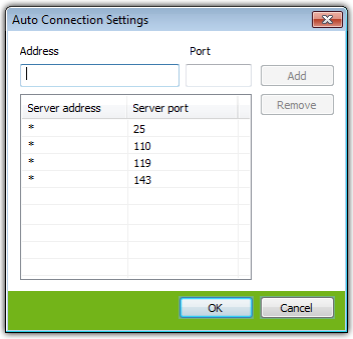
Interception Page

By default, **SpIDer Mail** automatically intercepts e-mail traffic of all user applications on your computer. You can disable mail traffic scanning for certain programs on the **Exclusions** page. For this, add the necessary applications to the list of exclusions.

The interception parameters of connections are set up on the **Interception** page.



By default, interception is carried out automatically. The list of intercepted addresses can be viewed in an additional window. To open it, click the **Parameters** button.



By default, the list of automatically intercepted messages includes all IP addresses (specified by the asterisk * symbol) and the following ports: 143 (standard IMAP4 port), 119 (standard NNTP port), 110 (standard POP3 port) and 25 (standard SMTP port).

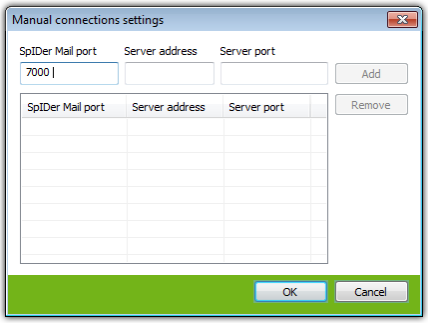
To remove an element from the list, select it and click the **Delete** button.

To add a server or a group of servers to the list, specify its address (IP address or domain name) in the **Address** field and the called port number into the **Port** field and click **Add**.

The **localhost** address is not intercepted if the asterisk (*) is specified. If necessary, this address should be specified in the interception list explicitly.

To set up manual interception

1. On the previously mentioned **Interception** page for setting up the mode of interception select the **Manual connections setup** radio button and click the **Parameters** button. A window for setting up manual connections will open.



2. Make up a list of resources (POP3/SMTP/IMAP4/NNTP servers) connections to which should be intercepted. Number them one after another starting from 7000. Hereinafter these numbers will be called **SpIDer Mail ports**.
3. For every resource input the appropriate number into the **SpIDer Mail** port entry field, a domain name or IP address of the server into the **Server address** entry field and the port number to which a connection is made into the **Server port** entry field and click the **Add** button.
4. Repeat these actions for each resource.
5. Click **OK**.

In the settings of the mail client, instead of the address and port of POP3/SMTP/IMAP4/NNTP server, specify the address localhost: port_SpIDer_Mail, where port_SpIDer_Mail is the address assigned to an appropriate POP3/SMTP/IMAP4/NNTP server.

Dr.Web for Outlook

General Functions

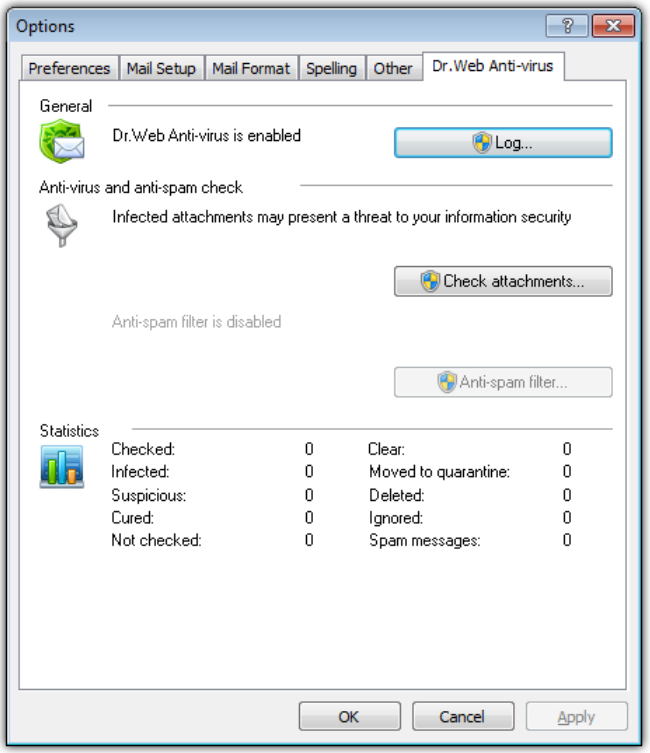
Dr.Web for Outlook plug-in performs the following functions:

- Anti-virus check of e-mail attachments transferred via SMTP, POP3 and HTTP protocols.
- Check of e-mail attachments transferred via SSL encrypted connections.
- Detection and neutralizing of malicious objects.
- Malware detection.
- Heuristic analysis for additional protection against unknown viruses.

Dr.Web for Outlook Plug-In Configuring

You can set up the parameters of the plug-in operation and review the statistics at the Microsoft Outlook mail application, in the **Service** → **Parameters** → **Dr.Web Anti-virus** tab (in the **Tools** → **Options** → **Dr.Web Anti-virus** tab for Microsoft Outlook 2007).

The **Dr.Web Anti-virus** tab of Microsoft Outlook parameters are active only if user has permissions to change these settings.



On **Dr.Web Anti-Virus** tab, the current protection status is displayed (enabled/disabled) and it provided the access to the following program functions:

- Log – allows to configure the program logging.
- Check attachments – allows to configure the e-mails check and to specify the program actions for the detected malicious objects.
- Statistics – allows to review the number of checked and processed objects.

Virus Check

Dr.Web for Outlook uses different detection methods. The infected objects are processed according to the actions defined by user: the program can cure the infected objects, remove them or move them to Quarantine to isolate them from the rest of the system.

Malicious Objects

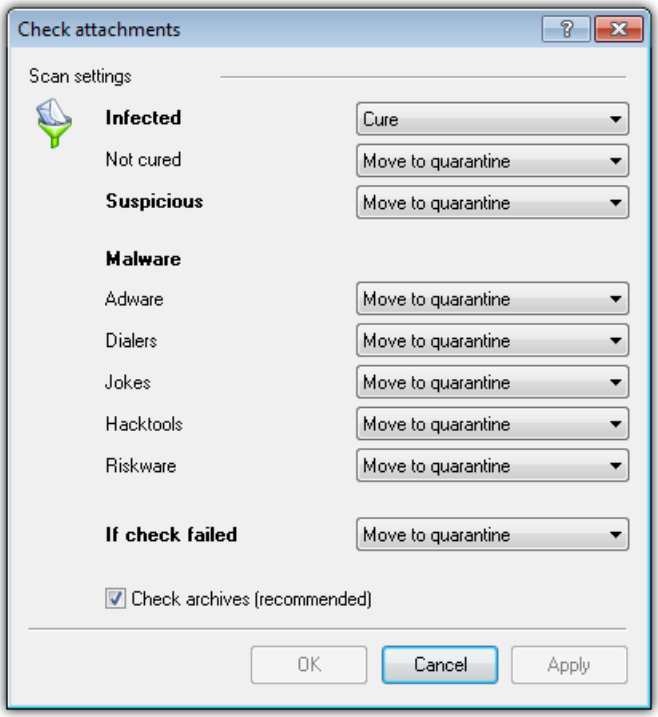
Dr.Web for Outlook detects the following malicious objects:

- Infected objects,
- Bomb viruses in files or archives,
- Adware,
- Hacktools,
- Dialer programs,
- Joke programs,
- Riskware;
- Spyware;
- Trojan horses (Trojans);
- Computer worms and viruses.

Actions

Dr.Web for Outlook allows to specify the program reaction to detection of infected or suspicious files and malicious objects during e-mail attachments check.

To configure the virus check of e-mail attachments and to specify the program actions for the detected malicious objects, in the Microsoft Outlook mail application, in the **Service** → **Parameters** → **Dr.Web Anti-virus** tab (in the **Tools** → **Options** → **Dr.Web Anti-virus** tab for Microsoft Outlook 2007), click **Check attachments**.



In the **Check attachments** window, specify the actions for different types of checked objects and also for the check failure. You can also enable/disable checking the archives.

To set actions on virus threats detection, use the following options:

- The **Infected** drop-down list sets the reaction to the detection of a file infected with a known virus.
- The **Not cured** drop-down list sets the reaction to the detection of a file infected with a known incurable virus (and in case an attempt to cure a file failed).
- The **Suspicious** drop-down list sets the reaction to the detection of a file presumably infected with a virus (upon a reaction of the heuristic analyzer).

- In the **Malware** section, set the reaction to the detection of types of unsolicited software such as:
  - Dialers;
  - Jokes;
  - Riskware;
  - Hakctools.
- The **If checked failed** drop-down list allows to configure actions, if attachment can not be checked, e.g. if attached file is corrupted of password protected.
- The **Check archives (recommended)** flag allows to enable or disable checking of attached archived files. Set this flag, to enable checking, clear – to disable.

For different types of objects, actions are assigned separately.

The following actions for detected virus threats are provided:

- **Cure** (only for infected objects) – instructs to try to restore the original state of an object before infection.
- **As incurable** (only for infected objects) – means, that the action specified for incurable objects will be performed.
- **Delete** – delete the object.
- **Move to quarantine** – move the object to the special Quarantine folder.
- **Skip** – skip the object without performing any action or displaying a notification.

Logging

Dr.Web for Outlook registers errors and application events in the following logs:

- Windows Event Log;
- Text Dr.Web debug log.

Event Log

Dr.Web for Outlook registers the following information in the Windows Event Log:

- Plug-in starts and stops.
- License key file parameters: license validation, license expiration date (information is written during program launch, during program operating and when key file is changed).
- License errors: the key file is absent, permissions for usage of program modules is absent in the key file, licence is blocked, the key file is corrupted (information is written during program launch and during program operating).
- Parameters of program modules: Scanner, engine, virus bases (information is written during program launch and modules update).
- Information on threats detection.
- License expiration notifications (a message is registered in 30, 15, 7, 3, 2 and 1 days before expiration).

To view Event Log

1. On the **Control Panel**, select **Administrative Tools** → **Event Viewer**.
2. In the tree view, select **Application**. The list of events, registered in the log by user applications, will be opened. The source of **Dr.Web for Outlook** messages is the **Dr.Web for Outlook** application.

Debug Text Log

The following information can be registered in the **Dr.Web for Outlook** text log:

- License validity status.
- Malware detection reports per each detected malicious object.
- Read-write errors or errors while scanning for archives or password-protected files.
- parameters of program modules: Scanner, engine, virus bases
- Core failures.
- License expiration notifications (A message is registered in 30, 15, 7, 3, 2 and 1 days before expiration).

Enabling the program logging in the Log file decreases server performance, therefore it is recommended to enable logging only in case of errors occurrence in operation of **Dr.Web for Outlook**.

Configure logging

1. On **Dr.Web Anti-virus** tab, click **Log**. The window of log settings will open.
2. Specify the detailing level (0 - 5) for logging:
   - level **0** corresponds to disable logging,
   - level **5** means the maximum level of details for the program logging.

   By default, logging is disabled.
3. Specify the maximum log file size (in kilobytes).
4. Click **OK** to save changes.

View program log

To open the text log, click **Show in folder**.

Statistics

In the Microsoft Outlook mail application, in the **Service** → **Parameters** → **Dr.Web Anti-virus** tab (in the **Tools** → **Options** → **Dr.Web Anti-virus** tab for Microsoft Outlook 2007), statistic information about total number of objects, which have been checked and treated by the program is listed.

These scanned objects are classified as follows:

- **Checked** – total number of checked messages.
- **Infected** – number of messages with viruses.
- **Suspicious** – number of messages presumably infected with a virus (upon a reaction of the heuristic analyzer).
- **Cured** – number of objects successfully cured by the program.
- **Not checked** – number of objects, which can not be checked or error has occurred during scan.
- **Clear** – number of messages, which are not infected.

Then the number of the following categories of treated objects is specified:

- **Moved to quarantine** – number of objects, which have been moved to Quarantine.
- **Deleted** – number of objects, deleted from the system.
- **Skipped** – number of objects, skipped without changes.

By default, statistics file is `drwebforoutlook.stat` file that is located in the %USERPROFILE%\DoctorWeb folder (for Windows 7, C:\Users\<*username*>\DoctorWeb). To clear statistics, delete this file.

`drwebforoutlook.stat` statistics file is individual for each system user.

Dr.Web Firewall

Dr.Web® Firewall protects your computer from unauthorized access and prevents leak of vital data through networks.

Dr.Web Firewall monitors connection attempts and data transfer and helps you block unwanted or suspicious connections both on network and application levels.

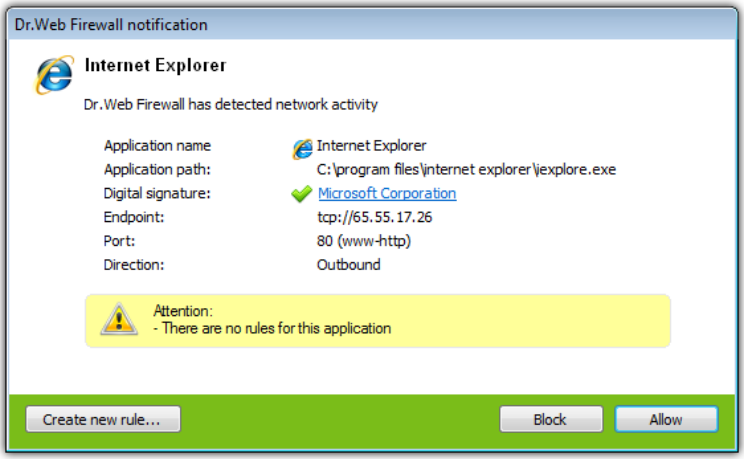
Main Features

Dr.Web Firewall provides you with the following features:

- Control and filtration of all incoming and outgoing traffic
- Access control on application level
- Network level packet filtering
- Fast selection of rule sets
- Event logging

Training Dr.Web Firewall

By default, once installation completes **Dr.Web Firewall** starts learning usual behaviour of your operating system by intercepting all new (unknown to the firewall) connection attempts and prompting you to select the necessary action.



You can either select a temporary solution, or create a rule which will be applied each time **Dr.Web Firewall** detects this type of connection.

When running under limited user account (Guest) **Firewall** does not prompt requests for network access attempts. Notifications are then forwarded to the session with administrator privileges, if such session is simultaneously active.

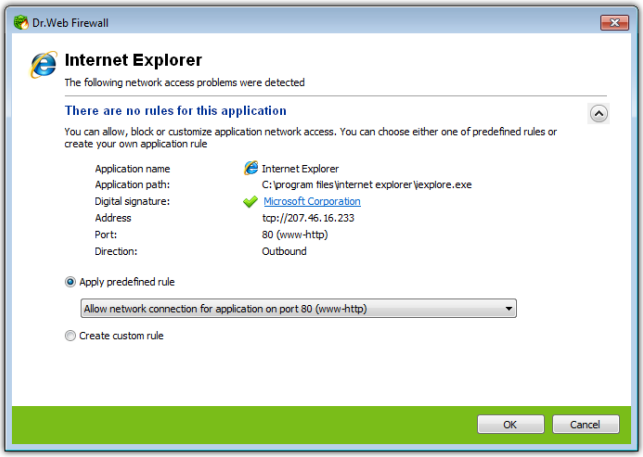
To process connection attempts

1. To make a decision, consider the following information displayed in the notification:

Information	Description
Application name	The name of the application. Ensure that the **Path** to the application executable file corresponds to its usual location.
Application path	The full path to the application executable file and its name.
Digital signature	Digital signature of the application.

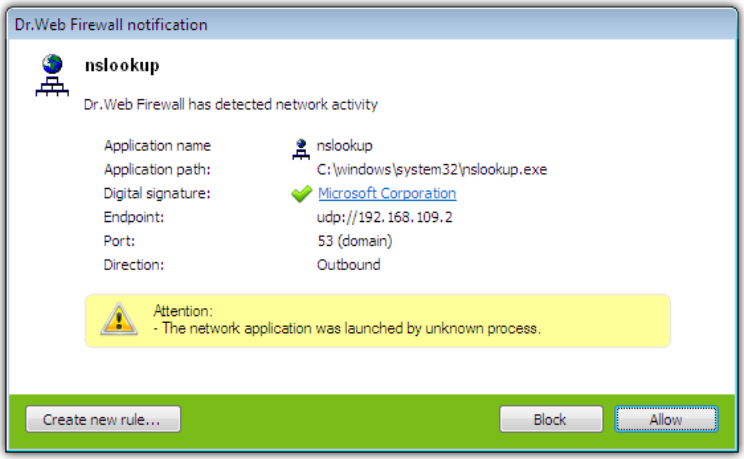
Information	Description
Endpoint	The protocol used and the network address the application is trying to connect to.
Port	The network ports used for the connection attempt.
Direction	Connection type.

2. Once you make a decision, select an appropriate action:
   - To block this connection once, select **Block**
   - To allow this connection once, select **Allow**
   - To open a window where you can create a new application filter rule, select **Create new rule**. In the opened window you can either choose one of the predefined rules or create your rule for application.



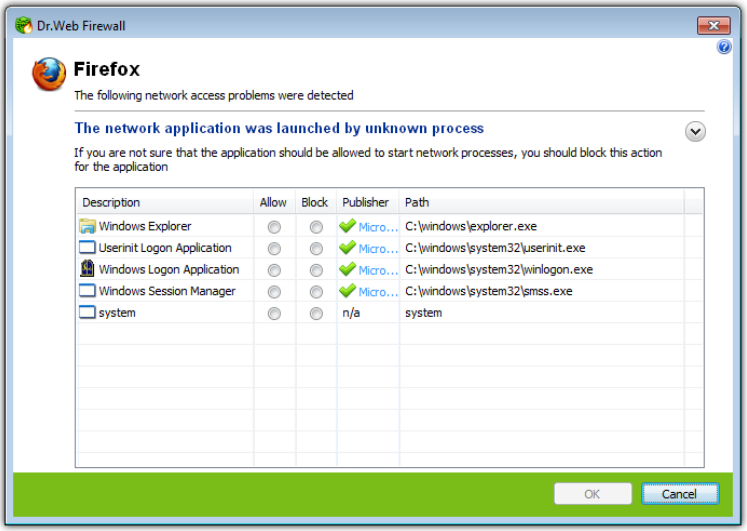
3. Click **OK**. **Dr.Web Firewall** executes the selected action and closes the notification window.

In cases when connection was initiated by a trusted application (an application with existing rules), but this application was run by an unknown parent process, a corresponding notification will be prompted:



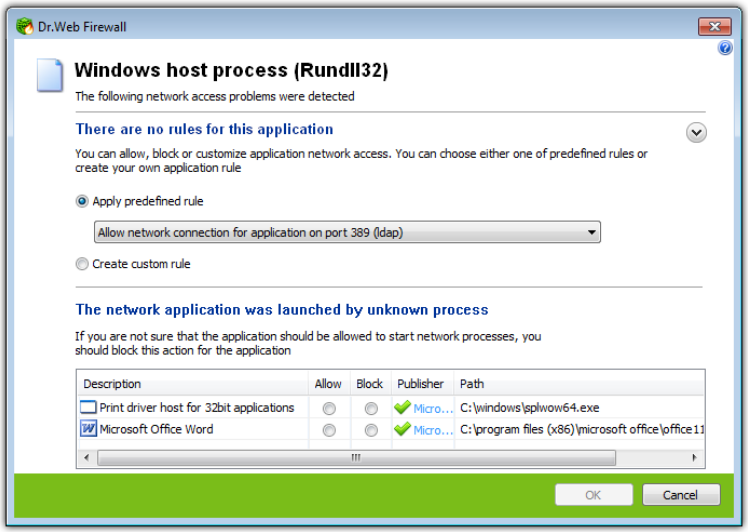
To set parent processes rules

1. Consider the information about parent process displayed in the notification.
   - To block this connection once, select Block
   - To allow this connection once, select **Allow**
   - To open a window where you can create a new application filter rule, select **Create new rule**. In the opened window you can either choose one of the predefined rules or create your rule for parent process.



2. Click **OK**. **Dr.Web Firewall** executes the selected action and closes the notification window.

When unknown process was run by another unknown process, a notification will display corresponding details. If you click **Create new rule**, the new window will appear, allowing you to create new rules for this application and it's parent process:


Dr.Web Firewall
Windows host process (Rundll32)
The following network access problems were detected
There are no rules for this application
You can allow, block or customize application network access. You can choose either one of predefined rules or create your own application rule
Apply predefined rule
Allow network connection for application on port 389 (ldap)
Create custom rule
The network application was launched by unknown process
If you are not sure that the application should be allowed to start network processes, you should block this action for the application
Description
Allow
Block
Publisher
Path
Print driver host for 32bit applications
Micro...
C:\windows\splwow64.exe
Microsoft Office Word
Micro...
C:\program files (x86)\microsoft office\office11
OK
Cancel

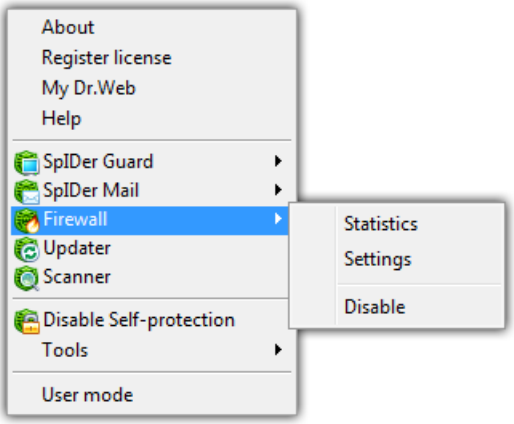
You need administrative rights to create rules.

Managing Dr.Web Firewall

Dr.Web Firewall installs as a network component and loads on Windows startup. If necessary, you can suspend **Dr.Web Firewall** operation, review its statistics, or change settings.

After a session under limited user account (Guest) is open **Firewall** displays an access error message. Firewall status is then displayed as inactive in **SpIDer Agent**. However, **Firewall** is enabled and operates with default settings or settings set earlier in administrative mode.

You can configure and manage **Dr.Web Firewall** using **SpIDer Agent**.



To manage Dr.Web Firewall

1. Right-click the **SpIDer Agent** icon .
2. Select **Firewall**, then select a required item:

Item	Select to
Statistics	Display information on events which **Dr.Web Firewall** handled.

Item	Select to
Settings	Access adjustable **Dr.Web Firewall** settings. On the **Restore Defaults** page you can restore all settings to their default values.
Disable	Suspend **Dr.Web Firewall** operation. This operation is available for users with administrative privileges only.
Enable	Resume **Dr.Web Firewall** operation. This item is available when **Dr.Web Firewall** is disabled only.

To disable **Dr.Web Firewall**, enter confirmation code.

Settings and **Disable**/**Enable** items are not available in **User mode**.

Firewall settings

You need administrative rights to access **Dr.Web Firewall** settings.

To start using **Dr.Web Firewall**, do the following:

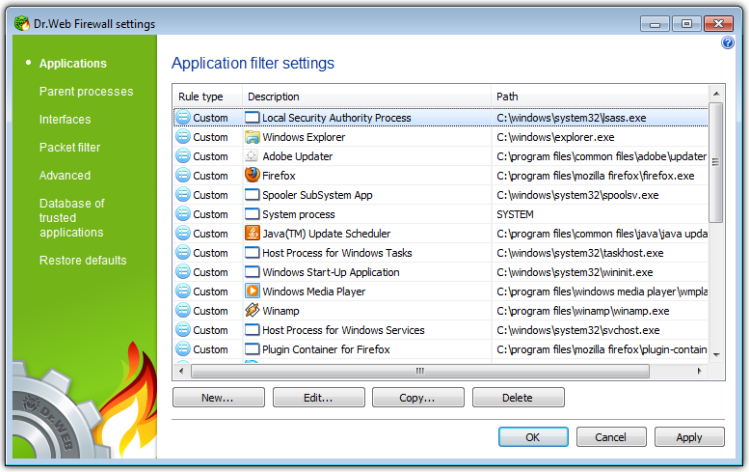
- Select operation mode
- List authorized applications

Dr.Web Firewall always loads on Windows startup and starts logging events. By default, **Dr.Web Firewall** operates in learning mode.

If any problems occur with Internet Connection Sharing (i.e. access to the Internet is blocked for computers that are connected to a host computer), on the host computer specify packet filter rule that allows all packets from the subnet, according to your local configuration.

Application Filter

Application level filtering helps you control access of various application and processes to network resources. You can create rules for both system and user applications.



The **Application filter settings** page lists all applications and processes for which there is an application filter rule set. Each application is explicitly identified by the path to its executable file. **Dr.Web Firewall** uses the SYSTEM name to indicate the rule set applied to the operating system kernel (the system process for which there is no unique executable file).

Dr.Web Firewall allows you to create no more than one set of rules per each application.

To configure rule sets

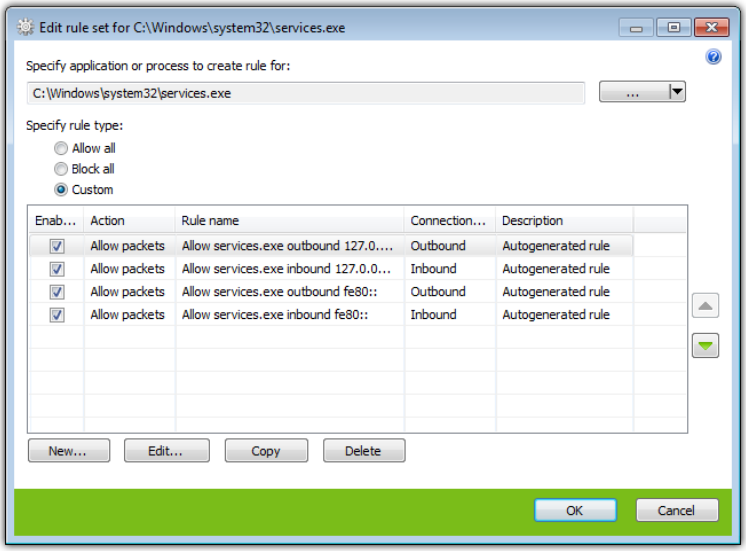
In the **Dr.Web Firewall** settings window, select the **Applications** page and do one of the following:

- to add a new set of rules, click **New**.
- to edit an existing set of rules, select the rule set in the list and click **Edit**.
- to add a copy of existing set of rules, select the rule set and click **Copy**. The copy is added after the selected rule set.
- to delete all rules for an application, select the appropriate rule set and click **Delete**.

If the application file, for which the rule was created, changes (e.g., due to update installation) then **Dr.Web Firewall** asks to confirm that the application is still allowed to access network resources.

Application Rules

The **New application rule set** (or **Edit rule set**) window lists types of the filtering rule for application or process, and also a rule set, if the **Custom** type is selected. You can change rule type, configure the list by adding new rules for the application or modifying existing rules and the order of their execution. The rules are applied according to their order in the set.



For each rule in the set, the following information displays:

Column	Description
Enabled	Execution states for the rule.
Action	The action for **Dr.Web Firewall** to perform when the connection attempt is detected: • **Block packets** • **Allow packets**
Rule name	The rule name.
Connection type	The party which initiates the connection: • **Inbound** – the rule is applied when someone from the network attempts to connect to the application on your computer. • **Outbound** – the rule is applied when the application on your computer attempt to connect to the network.

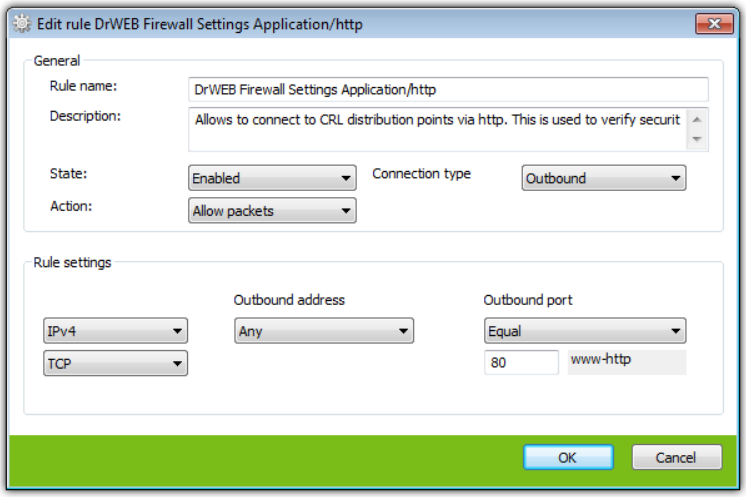
Column	Description
	• **Any** – the rule is applied regardless of who initiate the connection.
Description	The rule description.

To configure rules

1. If you select to create a new or edit an existing set of application filter rules on the **Application filter settings** page, in the opened window specify the application for which you want the rules to apply:
   - to add a set of rules for a user program, click and select the application executable file.
   - to add a set of rules for a process, click arrow on the button, choose **running application** and select the process.
2. Specify rule type:
   - **Allow all** – all connections will be allowed;
   - **Block all** – all connections will be blocked;
   - **Custom** – in this mode you can create a set of rules, that will allow or block different connections.
3. If you chose **Custom** type, create filtering rules using the following options:
   - to add a new rule, click **New**. The new rules is added to the end of the list.
   - to modify a rule, select it and click **Edit**.
   - to add a copy of a rule, select the rule and click **Copy**. The copy is added after the selected rule.
   - to delete a rule, select it and click **Delete**.
4. If you selected to create or edit a rule, configure rule settings in the opened window.
5. Use the arrows next to the list to change the order of rules. The rules are applied according to their order in the set.
6. When you finish adjusting the settings, click **OK** to save changes or **Cancel** to reject them.

Rule Settings

Application filtering rules control interaction of a particular application with certain network hosts.



To add or edit a rule

1. Configure the following parameters:

Parameter	Description
General	
Rule name	The rule name.
Description	The rule description.
State	One of the following execution states for the rule: • **Enabled** – apply rule for all matching connection attempts. • **Disabled** – do not apply the rule yet.
Connection type	The party which initiates the connection:

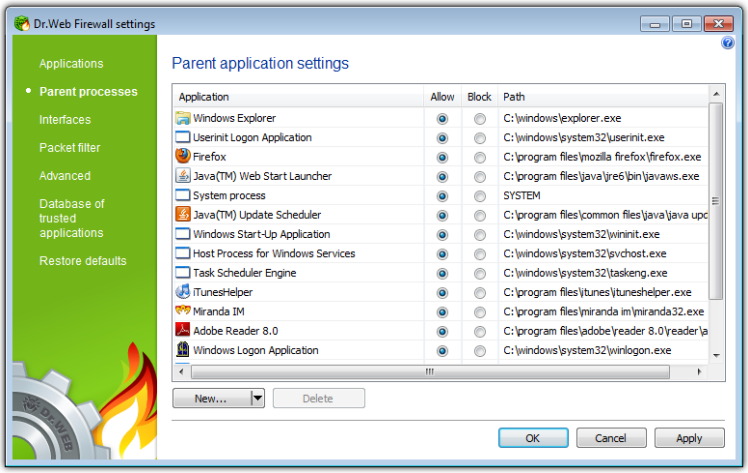
Parameter	Description
	• **Inbound** – apply the rule when someone from the network attempts to connect to the application on your computer. • **Outbound** – apply the rule when the application on your computer attempt to connect to the network. • **Any** – apply the rule regardless of who initiate the connection.
Action	The action for **Dr.Web Firewall** to perform when the connection attempt is detected: • **Block packets** • **Allow packets**
Rule Settings	
Protocol	The network and transport level protocols used for the connection attempt. **Dr.Web Firewall** supports the following network level protocols: • **IPv4** • **IPv6** • **IP all** – any version of IP protocol **Dr.Web Firewall** supports the following transport level protocols: • **TCP** • **UDP** • **TCP & UDP** – TCP or UDP protocol
Inbound/Outbound address	The IP address of the remote host. You can specify either a specific address (**Equals**) or several IP addresses using a range (**In range**), specific subnetwork mask (**Mask**), or masks of all subnetworks, in which your computer has network addresses (**MY_NETWORK**). To apply the rule for all remote hosts, select **Any**.

Parameter	Description
Inbound/Outbound port	The port used for connection. You can specify either a specific port number (**Equals**) or a port range (**In range**). To apply the rule for all ports, select **Any**.

2. When you finish adjusting the settings, click **OK** to save changes or **Cancel** to reject them.

Parent processes

To allow or forbid processes or applications to run other applications you have to set up appropriate rules on **Parent processes** page.



To add rule for parent process

1. Choose parent process:
   - to add new rule for an application click **New** and browse for program executable
   - to add new rule for an already running process click arrow on **New**, choose running application and select process
2. Set appropriate action:
   - **Block** to prevent application from running other processes
   - **Allow** to permit application to run other processes

   New process is blocked by default.

Packet Filter

Packet filtering allows you to control access to network regardless of which program initiates connection. **Dr.Web Firewall** applies these rules to network packets transmitted through network interfaces of your computer.

Packet filtering allows you to control access to networks on a lower level than the application filter thus providing you with more flexible options.

Dr.Web Firewall provides you the following default filtering rule sets:

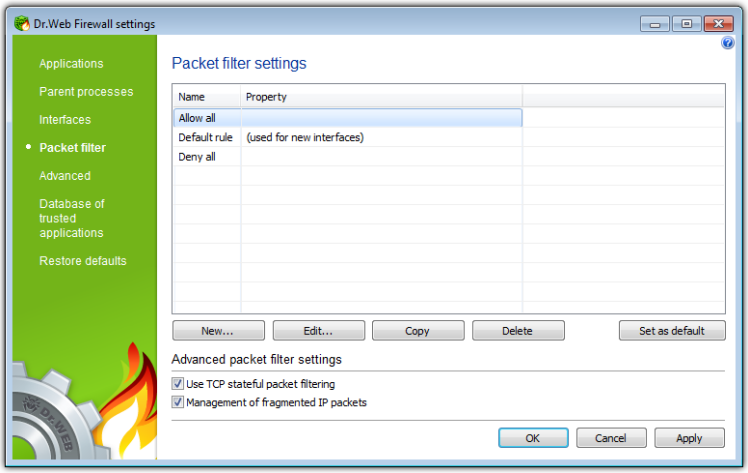
- **Allow all** – this rule set configures **Dr.Web Firewall** to pass through all packets.
- **Deny all** – this rule set configures **Dr.Web Firewall** to block all packets.
- **Default rule** – this set includes rules describing the most popular system configurations and preventing common network attacks. This rule set is used by default for new network interfaces.

For fast switching between filtering modes, you can create custom sets of filtering rules.

To set rulesets for network interfaces

In the **Dr.Web Firewall** settings window, select **Packet filter** page. On this page you can:

- Configure sets of filtering rules by adding new rules, modifying or deleting existing ones, or changing order of rules execution.
- Select a default filtering rule.
- Configure general filtering settings.



To configure sets of filtering rules

Do one of the following:

- to add a new rule set, click **New**. The new rule set is added to the beginning of the list.
- to edit an existing set of rules, select the rule set in the list and click **Edit**.
- to add a copy of existing set of rules, select the rule set and click **Copy**. The copy is added after the selected rule set.
- to delete a selected rule set, click **Delete**.

To set default rules

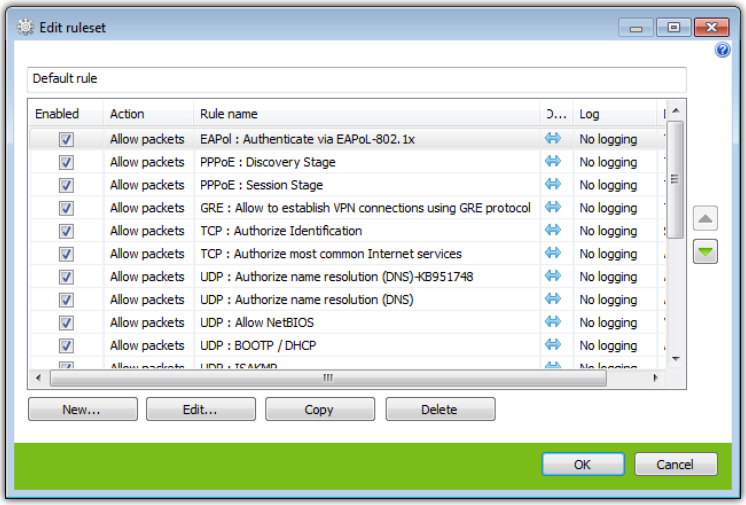
In the list, select the ruleset you want to use for new network interfaces installed on your computer and click **Set as default**.

To configure general settings

On the **Packet Filter settings**, use the following options:

Option	Description
Use TCP stateful packet filtering	Select this checkbox to filter packets according to the state of existing TCP connections. **Dr.Web Firewall** will block packets that do not match active connections according to the TCP protocol specification. This option helps protect your computer from DoS attacks (denial of service), resource scanning, data injection and other malicious operations. It is also recommended to enable stateful packet filtering when using complex data transfer protocols such as FTP, SIP, etc. Clear this checkbox to filter packets without regard to state of TCP sessions.
Management of fragmented IP packets	Select this checkbox to ensure correct processing of large amounts of data. The maximum transmission unit (MTU) may vary for different networks, therefore large IP packets may be received fragmented. When this option is enabled, **Dr.Web Firewall** applies the rule selected for the first fragment of a large IP packet to all other fragments. Clear this checkbox to process fragmented packets independently.

The **New packet ruleset** (or **Edit ruleset**) window lists packet filtering rules for the selected rule set. You can configure the list by adding new rules for the application or modifying existing rules and the order of their execution. The rules are applied according to their order in the set.



For each rule in the set, the following information displays:

Column	Description
Enabled	Execution states for the rule.
Action	The action for **Dr.Web Firewall** to perform when the packet is intercepted: • **Block packets** • **Allow packets**
Rule name	The rule name.
Direction	The packet sender: • – the rule is applied when packet is received from the network. • – the rule is applied when packet is sent into the network from your computer. • – the rule is applied regardless of packet transfer direction.
Log	The logging mode for the rule. This parameter defines which information is stored in the **Dr.Web Firewall** log:

Column	Description
	• **Log headers** – the packet header only. • **Entire packet** – the whole packet. • **No logging** - no information is logged.
Description	The rule description.

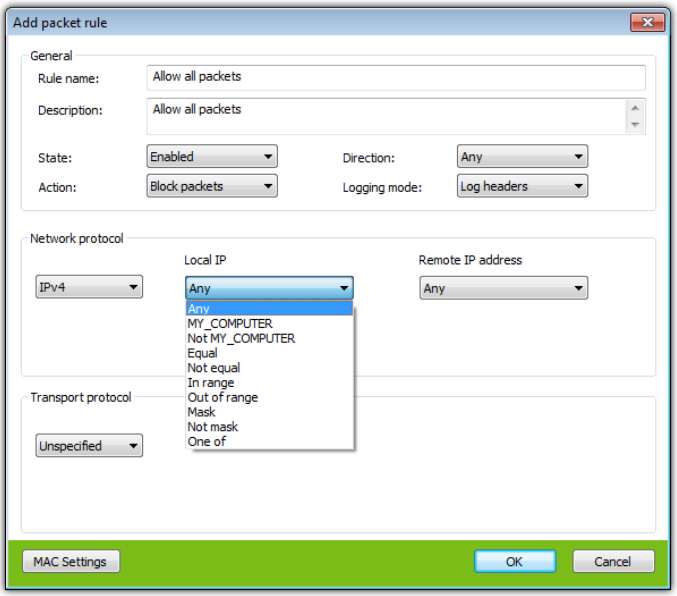
You can configure the list by adding new rules for the application or modifying existing rules and the order of their execution. The rules are applied according to their order in the set.

To configure rulesets

1. If you select to create or edit an existing rule set on the **Packet filtering settings** page, in the opened window, specify the name for the rule set.
2. Use the following options to create filtering rules:
   - to add a new rule, click **New**. The new rules is added to the beginning of the list.
   - to modify a rule, select it and click **Edit**.
   - to add a copy of a rule, select the rule and click **Copy**. The copy is added after the selected rule.
   - to delete a rule, select it and click **Delete**.
3. If you selected to create or edit a rule, configure rule settings in the opened window.
4. Use the arrows next to the list to change the order of rules. The rules are applied according to their order in the set.
5. When you finish adjusting the settings, click **OK** to save changes or **Cancel** to reject them.

To add or edit a rule

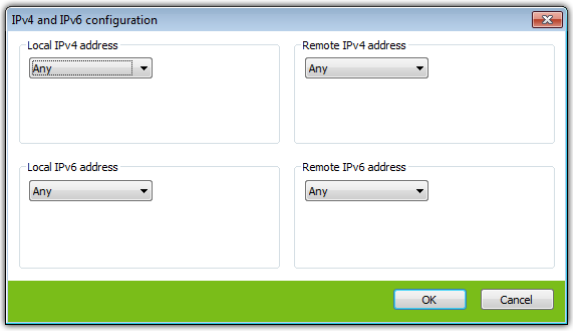
1. In the packet filter rule set creation or modification window, click **New** or **Edit**. This opens a rule creation or rule modification window.

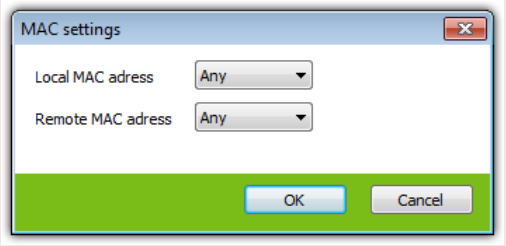


2. Configure the following parameters:

Parameter	Description
General	
Rule name	The rule name.
Description	The rule description.
State	One of the following execution states for the rule: • **Enabled** – apply the rule for all matching packets. • **Disabled** – do not apply the rule yet.
Direction	The packet sender: • **Inbound** – apply the rule when packet is received from the network.

Parameter	Description
	• **Outbound** – apply the rule when packet is sent into the network from your computer. • **Any** – apply the rule regardless of packet transfer direction.
Action	The action for **Dr.Web Firewall** to perform when the packet is intercepted: • **Block packets** • **Allow packets**
Logging mode	The logging mode for the rule. This parameter defines which information is stored in the **Dr.Web Firewall** log: • **Log headers** – log packet headers only. • **Entire packet** – log whole packets. • **No logging** – do not log any information.
Network Level Protocol	
Protocol	Select one of the following network level protocols: • **IPv4** - Internet Protocol version 4 • **IPv6** - Internet Protocol version 6 • **IP all** - Internet Protocol of any version • **ARP** - Address Resolution Protocol • **EAPoL-802.1x** - Extensible Authentication Protocol (the IEEE 802.1X standard) • **PPPoE Discovery** • **PPPoE Session** To apply the rule for all protocols, select **Unspecified**.
Local IP	(Available for **IPv4**, **IPv6**, or **IP all** protocols only) Select the comparison method and enter the IP address of your computer.
Remote IP	(Available for **IPv4** or **IPv6** protocols only) Select the comparison method and enter the IP address of the remote host.
Change	(Available for **IP all** protocol only) Click to view the IP protocols configuration window.

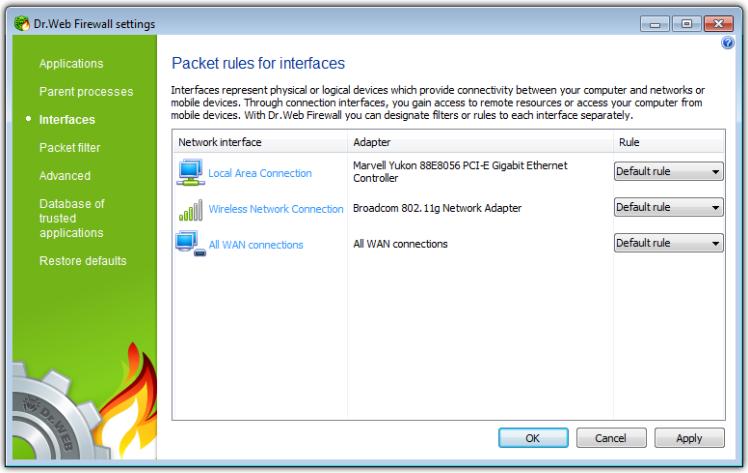
Parameter	Description
	 Configure the following parameters: • **Local IPv4 address** – select the comparison method and enter your IPv4 address. • **Remote IPv4 address** – select the comparison method and enter the IPv4 address of the remote host. • **Local IPv6 address** – select the comparison method and enter your IPv6 address. • **Remote IPv6 address** – select the comparison method and enter the IPv6 address of the remote host.
Transport Level Protocol	
Protocol	Select one of the following transport level protocols: • **TCP** • **UDP** • **ICMPv4** – available for the IPv4 network level protocol only. • **ICMPv6** – available for the IPv6 network level protocol only. • **IGMP** – available for the IPv4 network level protocol only. • **GRE** – available for the IPv4 network level protocol only. • **SIPP-ESP** To apply the rule for all protocols, select **Unspecified**.

Parameter	Description
	For **ARP** or **EAPoL-802.1x** protocols, you cannot select a transport level protocol (**Unspecified**).
MAC Settings	Click to view MAC address filtering options.  Configure the following parameters: • **Local MAC address** – the MAC address of your network card. • **Remote MAC address** – the MAC address of the remote computer.

3. When you finish adjusting the settings, click **OK** to save changes or **Cancel** to reject them.

Network Interfaces

On the **Interfaces** page you can select a rule set to use for filtering packets transmitted through different network interfaces.


Dr.Web Firewall settings
Applications
Parent processes
Interfaces
Packet filter
Advanced
Database of trusted applications
Restore defaults
Packet rules for interfaces
Interfaces represent physical or logical devices which provide connectivity between your computer and networks or mobile devices. Through connection interfaces, you gain access to remote resources or access your computer from mobile devices. With Dr.Web Firewall you can designate filters or rules to each interface separately.
Network interface
Adapter
Rule
Local Area Connection
Marvell Yukon 88E8056 PCI-E Gigabit Ethernet Controller
Default rule
Wireless Network Connection
Broadcom 802.11g Network Adapter
Default rule
All WAN connections
All WAN connections
Default rule
OK
Cancel
Apply

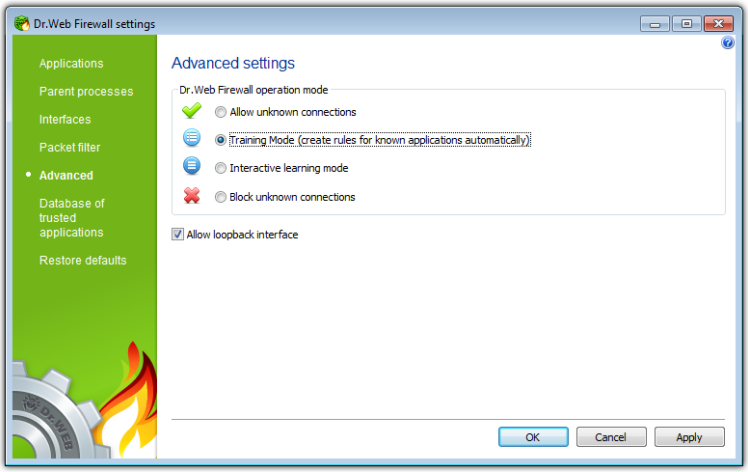
On the **Packet rules for interfaces** page, you can select a packet filtering ruleset to use for each network interface installed on your computer.

To set rulesets for network interfaces

1. In the **Dr.Web Firewall** settings window, select **Interfaces**.
2. For an interface of interest, select the appropriate ruleset. If a ruleset does not exist, you can create a new set of packet filtering rules.
3. Click **OK** to save changes, or click **Cancel** to close the window without saving changes.

Advanced settings

On the **Advanced settings** page, you can select a default action, which **Dr.Web Firewall** should execute when it detects a new (unknown to the firewall) connection attempt, and configure advanced settings. These rules are applied on the application level.



To set operation mode

1. In the **Dr.Web Firewall** settings window, select **Mode**.
2. Select one of the following operation modes:
   - Interactive learning mode
   - (Default) **Training mode (create rules for known applications automatically)** – learning mode, when rules for known applications are created automatically.
   - **Block unknown connections** – restricted access mode, when all unknown connections are blocked. For known connections, **Dr.Web Firewall** applies the appropriate rules.
   - **Allow unknown connections** – free access mode, when all unknown applications are permitted to access networks.

3. Click **OK** to save changes, or click **Cancel** to close the window without saving changes.

Learning Mode

In this mode, you have total control over **Dr.Web Firewall** reaction on unknown connection detection, thus training the program while you working on computer.

When a user application or operating system attempts to connect to a network, **Dr.Web Firewall** checks if there is a filtering rule set for the application. If there are no filtering rules, **Dr.Web Firewall** prompts you to select a temporary solution, or create a rule which will be applied each time **Dr.Web Firewall** detects this type of connection.

Training Mode

In this mode, rules for known applications are created automatically. For other apllications you have control over **Dr.Web Firewall** reaction.

When a user application or operating system attempts to connect to a network, **Dr.Web Firewall** checks if there is a filtering rule set for the application. If there are no filtering rules, **Dr.Web Firewall** prompts you to select a temporary solution, or create a rule which will be applied each time **Dr.Web Firewall** detects this type of connection.

This mode is used by default.

Restricted Access Mode

In this mode, **Dr.Web Firewall** blocks all unknown connections to network resources including the Internet automatically.

When a user application or operating system attempts to connect to a network, **Dr.Web Firewall** checks if there is a filtering ruleset for the

application. If there are no filtering rules, **Dr.Web Firewall** blocks network access for the application without displaying any notification to the user. If there are filtering rules for the application, **Dr.Web Firewall** processes the connection according to the specified actions.

Free Access Mode

In this mode, **Dr.Web Firewall** allows all unknown applications to access network recourses including the Internet. No notification on access attempt is displayed.

To configure advanced settings

On the **Application filter settings** page, use the following option:

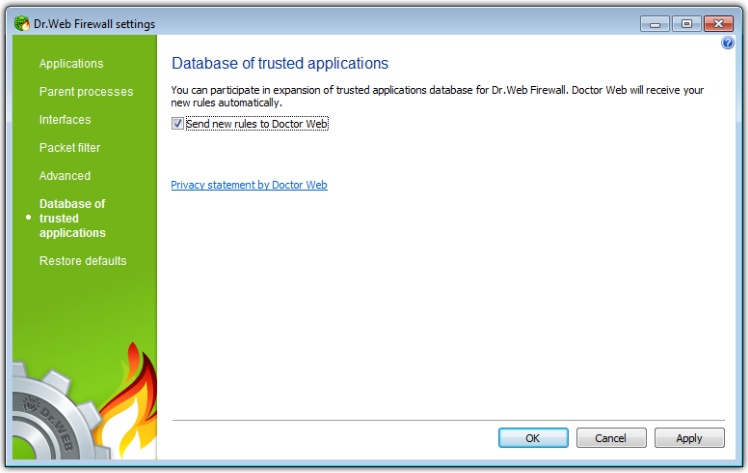
Option	Description
Allow loopback interface	Select this checkbox to allow all applications on you computer to interconnect (i.e. allow unlimited connections between application installed on your computer). For this type of connection, no rules will be applied. Clear this checkbox to apply rules for connections carried out both through the network and within your computer.

Database of trusted applications

You can participate in expansion of trusted applications database for **Dr.Web Firewall**.

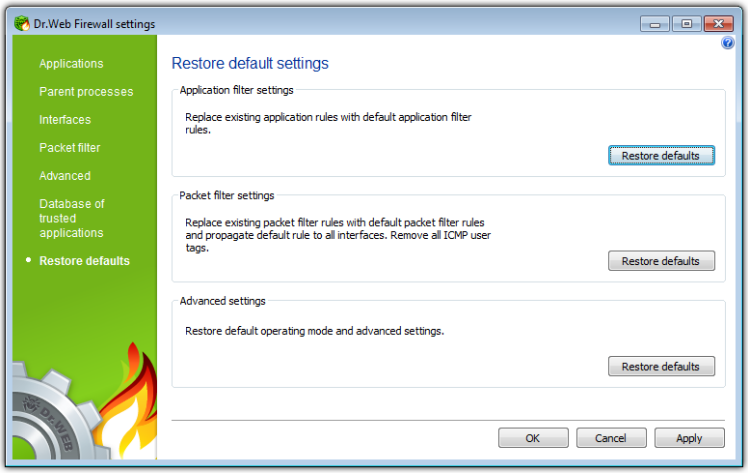
Select the **Send new rules to Doctor Web** checkbox to allow **Dr.Web Firewall** to send created rules to **Doctor Web**.

Click the **Privacy statement by Doctor Web** link to look through a privacy statement on **Doctor Web** website.



Restoring Defaults

On the **Restore default settings** page, you can restore **Dr.Web Firewall** settings to their default values recommended by **Doctor Web**.



To restore default settings

1. In the **Dr.Web Firewall** settings window, select **Restore defaults**.
2. Do one of the following:
   - To restore default application filter settings, in the **Application filter settings** section, click **Restore defaults**.
   - To restore default packet filter settings, in the **Packet filter settings** section, click **Restore defaults**.
   - To set the default **Dr.Web Firewall** operation mode, in the **Advanced settings** section, click **Restore defaults**.
3. Click **OK** to save changes, or click **Cancel** to close the window without saving changes.

Event Logging

Dr.Web Firewall registers connection attempts and network packets in the following logs:

- Application Filter Log (**Application journal**), which contains information on network connection attempts from various applications and rules applied to process each attempt.
- Packet Filter Log (**Packet Filter journal**), which contains information on network packets processed by **Firewall**, rules applied to process the packets, and network interfaces used to transmit the packets. Details level depends on settings of each packet application rule.

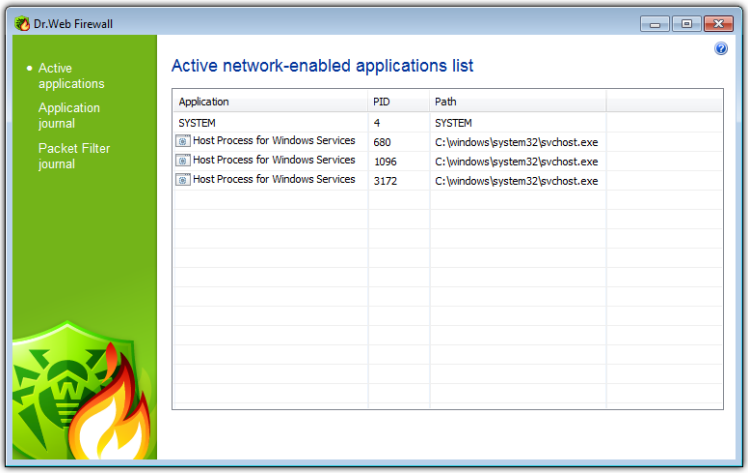
The **Active applications** page displays applications currently connected to a network.

To open journals

1. Click the **SpIDer Agent** icon .
2. Select **Firewall**, then select **Statistics**.

Active Applications

The list of active applications displays information on programs accessing network resources at the moment.

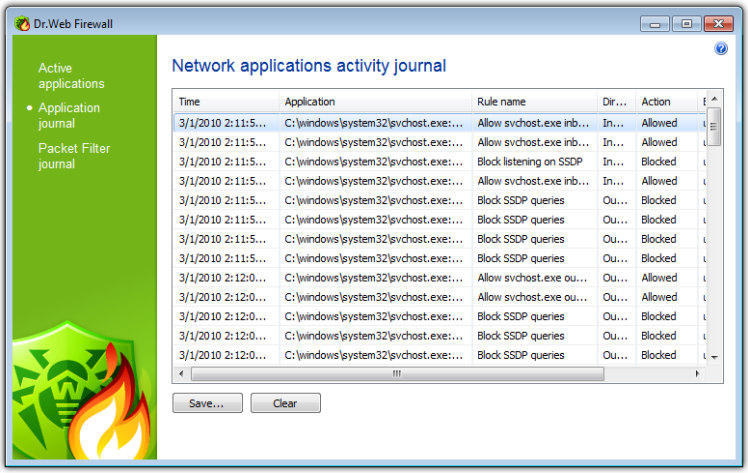


Column	Description
Application	The application description if available in the operating system.
PID	The identification number of the application process.
Path	The full path to the application executable file.

If necessary, use the process PID to terminate the application manually.

Application Filter Log

The application filter log stores information on all attempts of applications installed on your computer to connect to a network.


Dr.Web Firewall
Active applications
Application journal
Packet Filter journal
Network applications activity journal
Time
Application
Rule name
Dir...
Action
3/1/2010 2:11:5... C:\windows\system32\svchost.exe:... Allow svchost.exe inb... In... Allowed
3/1/2010 2:11:5... C:\windows\system32\svchost.exe:... Allow svchost.exe inb... In... Allowed
3/1/2010 2:11:5... C:\windows\system32\svchost.exe:... Block listening on SSDP In... Blocked
3/1/2010 2:11:5... C:\windows\system32\svchost.exe:... Allow svchost.exe inb... In... Allowed
3/1/2010 2:11:5... C:\windows\system32\svchost.exe:... Block SSDP queries Ou... Blocked
3/1/2010 2:11:5... C:\windows\system32\svchost.exe:... Block SSDP queries Ou... Blocked
3/1/2010 2:11:5... C:\windows\system32\svchost.exe:... Block SSDP queries Ou... Blocked
3/1/2010 2:11:5... C:\windows\system32\svchost.exe:... Block SSDP queries Ou... Blocked
3/1/2010 2:12:0... C:\windows\system32\svchost.exe:... Allow svchost.exe ou... Ou... Allowed
3/1/2010 2:12:0... C:\windows\system32\svchost.exe:... Allow svchost.exe ou... Ou... Allowed
3/1/2010 2:12:0... C:\windows\system32\svchost.exe:... Block SSDP queries Ou... Blocked
3/1/2010 2:12:0... C:\windows\system32\svchost.exe:... Block SSDP queries Ou... Blocked
3/1/2010 2:12:0... C:\windows\system32\svchost.exe:... Block SSDP queries Ou... Blocked
Save...
Clear

Column	Description
Time	The date and time of the connection attempt.
Application	The full path to the application executable file, its name and process identification number (PID).
Rule name	The name of the rule applied.
Direction	The party which initiated the connection: • **Inbound** – someone from the network attempted to connect to the application on you computer. • **Outbound** – the application on your computer attempted to connect to the network. • **Any** – the rule was applied regardless of who initiated the connection.
Action	The action **Dr.Web Firewall** performed when the connection attempt was detected:

Column	Description
	• **Block packets** • **Allow packets**
Endpoint	The protocol, IP-address and the port used for the connection.

On this page you can save the information to a file or clear the log.

To save application filter log

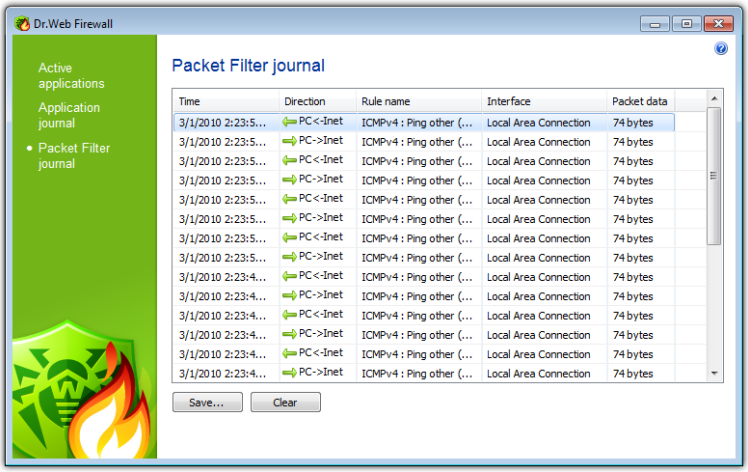
Click **Save**, then enter the file name where to store the log.

To clear application filter log

Click **Clear**. All information will be deleted from the log.

Packet Filter Log

The packet filter log stores information on packets transmitted through all network interfaces installed on you computer, if **Log headers** or **Entire packet** logging mode was set for these packets. If **No logging** mode was set for a packet, no information is stored.



Column	Description
Time	The date and time when the packet was processed.
Direction	The packet sender: • – the packet was transmitted from the network to your computer. • – the packet was transmitted from your computer to the network. • – the packet sent from the network to your computer was blocked. • – the packet sent from your computer to the network was blocked.
Rule name	The name of the applied rule.

Column	Description
Interface	The interface used to transmit the packet.
Packet data	Packet details. The **Logging mode** setting of the rule determines the amount of stored data.

On this page you can save the information to a file or clear the log.

To save packet filter log

Click **Save**, then enter the file name where to store the log.

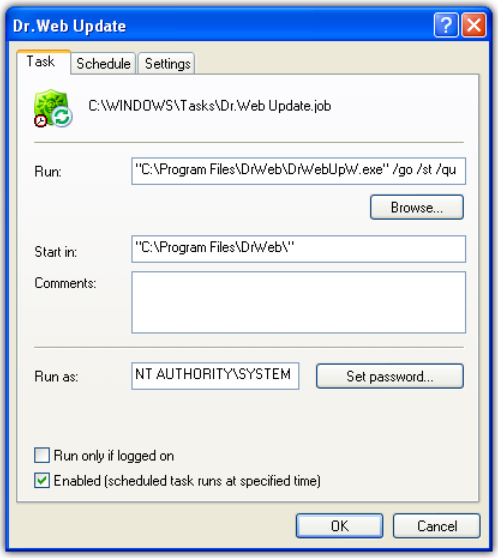
To clear packet filter log

Click **Clear**. All information will be deleted from the log.

Automatic Launch of Tasks for Scanning and Updating in Dr.Web

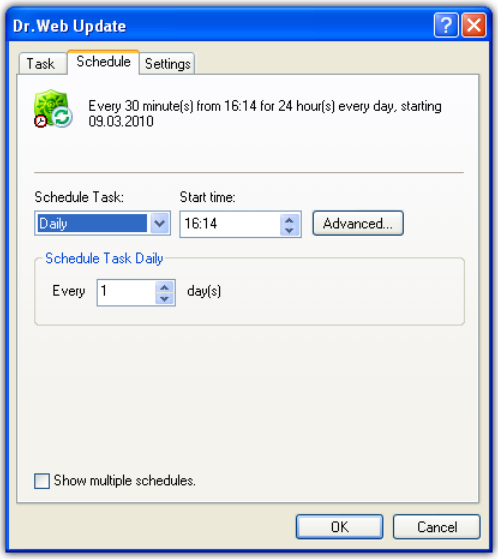
During **Dr.Web Anti-virus** installation a task to update the virus databases and other files of the package is automatically created in the system scheduler (the Scheduled Tasks directory). To view the parameters of this task, select **Scheduler** in the **Tools** submenu of **SpIDer Agent** context menu. Settings for Windows XP are described below.

In Windows Vista/7 the **Scheduler** item will open Task Scheduler.

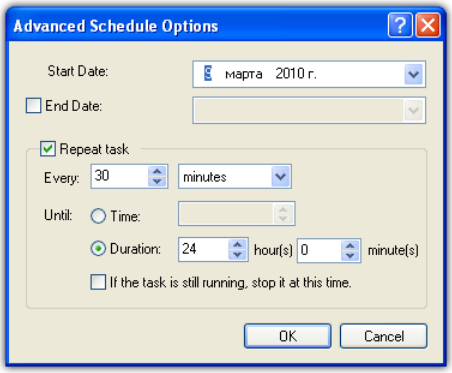


In the **Task** tab the full name of the executable file and the command line parameters of the task are specified. The **Enabled** check box instructs to perform the task (if the check box is cleared the task is saved to the folder, but is not performed).

In the **Schedule** tab the schedule according to which a task will be run automatically is made.



Click **Advanced**. The **Advanced Schedule Options** window will open.



If installed components include **Dr.Web Firewall**, Task Scheduler (**Scheduler** item) will be blocked by **Firewall** after **Dr.Web Anti-virus** installation and the first system reboot. Scheduled tasks will operate only after second restart when new rule is already created.

You can set your own tasks for anti-virus updating and scanning, delete or edit tasks. Consult the Help system and Windows documentation for more details on the system scheduler operation.

Automatic Updating

Modern computer viruses are characterized by the high-speed distribution. Within several days, and sometimes hours, a newly emerged virus can infect millions of computers around the world.

Developers of the anti-virus constantly supplement the virus databases with new records. When such updates are installed, the anti-virus can detect new viruses, block their distribution and, in some cases, cure the infected files.

From time to time the anti-virus algorithms implemented as executable files and program libraries are being updated. The field experience of the anti-virus helps to correct the detected program errors; the help system and documentation are being improved.

To speed up and facilitate the receipt and installation of the virus database updates and other files a special component – **Dr.Web Automatic Updating Utility for Windows** (**Updater**) – was created.

General Information

The operation of the **Updater** is governed by the structure of the virus databases and by the method of updating the virus databases and the program on the whole:

- The program includes the main virus database (drwebase.vdb) and its extensions (files drw50000.vdb, drw50001.vdb, drw50002.vdb, drw50003.vdb and drw50004.vdb). They all contain virus signatures known at the moment of the release of the given version of the program (for more details on the version read below).
- Once in a week the weekly add-ons are released – these are files with the virus records for detection and neutralization of viruses detected since the previous week's add-on's release. The weekly add-ons are files which look like this: drwXXXYY.vdb, where XXX

is the current anti-virus version number (without a separating full stop), and YY is the number of the weekly add-on. The weekly add-ons are numbered beginning from 05, i.e. the first add-on of the database is called drw50005.vdb.

- If necessary (usually several times per day), hot add-ons with virus records for detection and neutralization of viruses detected since the last weekly add-ons are released. This add-on is the file called drwtoday.vdb. In the end of a day all the virus records from this file are included in drwdaily.vdb accumulative add-on. In the end of a weekend drwdaily.vdb contents are issued as the next weekly add-on.
- The program includes additional databases of malicious programs drwnasty.vdb and drwrisky.vdb. The records for detection of adware and dialers are included into the drwnasty. vdb virus database. The records for detection of joke programs, riskware and hacktools are included into the drwrisky.vdb virus database.
- From time to time cumulative add-ons for malicious programs database are released. Hot add-ons of these databases can be released much more rarely than for the main virus base.From time to time the updates of other files are released independently to the virus database updates.
- From time to time fundamental updates of the anti-virus protection programs are released. This is a new anti-virus version release. All the virus records known up to this moment are included into the new main virus database. Old virus databases are deleted when the new version is installed.

Thus, the structure of the virus databases will be as follows:

- the main virus database – drwebase.vdb
- extensions of the main virus database – drw50000.vdb, drw50001.vdb, drw50002.vdb, drw50003.vdb and drw50004.vdb
- weekly add-ons – drw50005.vdb, drw50006.vdb etc.
- hot add-on – drwtoday.vdb
- accumulative add-on – drwdaily.vdb
- additional databases of malicious programs – drwnasty.vdb and drwrisky.vdb
- cumulative add-ons to malicious programs database – dwn50001.vdb, dwn50002.vdb etc. and dwr50001.vdb,

dwr50002.vdb etc.

- hot add-ons of the additional databases of malicious programs – dwntoday.vdb and dwrtoday.vdb

The most convenient way to receive and install the updates of the virus databases and the program is to use the **Updater** described below.

To use the **Updater** you should have an Internet connection.

User should have administrator rights to update components of **Dr. Web**.

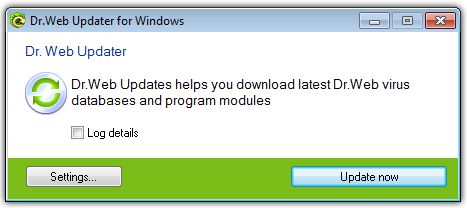
Launching and Using the Automatic Updating Utility

The **Automatic Updating Utility** (**Updater**) can be launched in one of the following ways:

- automatically, according to schedule (read Automatic Launch of Tasks for Scanning and Updating in Dr.Web);
- from the command line by activating the drwebupw.exe executable file from the program's installation folder;
- by selecting the **Update** item in the context menu of the **SpIDer Agent** icon;
- by selecting the **Update** item of the **File** menu in the main window of the **Scanner** (read Using Dr.Web Scanner for Windows);
- by pressing F8 in the active **Scanner** window.

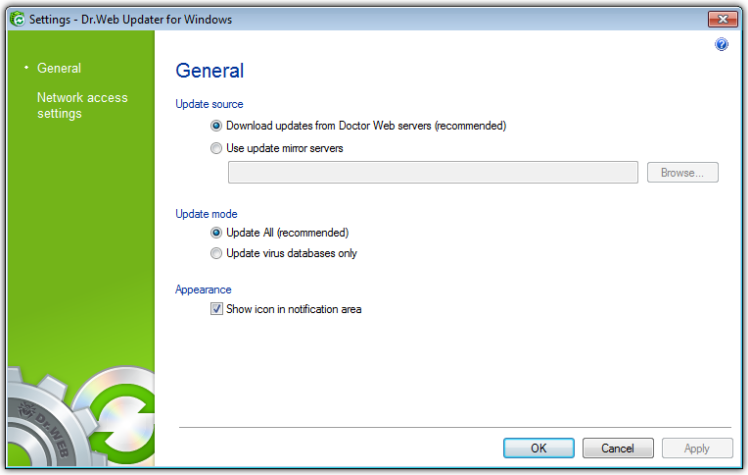
If you launch **Dr.Web Updater** from **SpIDer Agent** menu or from the command line, the dialog window will open. You can launch update or set necessary parameters. Also you can set the **Log details** flag to increase change log detail level. All changes are logged into drwebupw.log file, that is located in %USERPROFILE%\DoctorWeb folder (in Windows 7, C:\Users\<*username*>\DoctorWeb).

If launching **Dr.Web Updater** automatically, changes are logged into drwebupw.log file, that is located in the installation folder.


Dr.Web Updater for Windows
Dr. Web Updater
Dr.Web Updates helps you download latest Dr.Web virus databases and program modules
Log details
Settings...
Update now

Settings

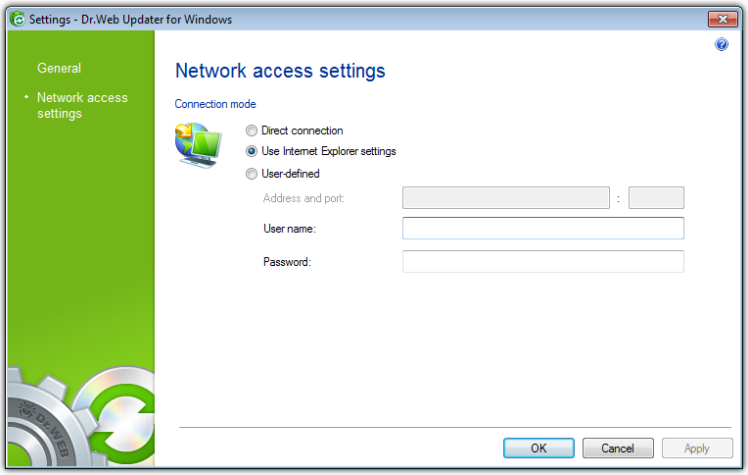
To adjust update settings press the **Settings** button.



On the **General** page you can set the following parameters:

- **Update source**. **Dr.Web Updater** can download updates from **Doctor Web** servers (recommended) or mirror servers. If you use mirrors, set up necessary parameters;
- **Update mode**. You can choose one of the following:
  - **Update all (recommended)**. In this mode all **Dr.Web Anti-virus** components, virus databases and anti-virus engine will be updated;
  - **Update virus databases only**. In this mode **Dr.Web Anti-virus** components will not be updated;
- **Appearance**. By default, notifications are displayed when update is finished. You can disable this option.

In the **Network access settings** page you can set up network access.



If you do not use a proxy server, choose **Direct connection**.

If you use current settings for proxy server, choose **Use Internet Explorer settings**.

If you want to specify settings for proxy server, choose **User defined** and set up necessary parameters.

When **Dr.Web Updater** starts automatically, direct connection to Internet is used, so Internet Explorer settings cannot be used. If you need to connect using proxy-server, specify required parameters in scheduled updating settings.

Launching Update

When launching update, the program checks the presence of the license key file in the installation folder, and, if it fails to find it, it tries to receive it via the Internet at www.drweb.com (this is described at the end of the License Key File section). If no key file is found, the updating is impossible.

If the key file is found, the program checks its validity at www.drweb.com (the file can be blocked, if discredited, i.e. its illegal distribution is uncovered). If the key file is blocked, the updating is not done; a correspondent message is generated to a user.

If the key is blocked, contact the dealer you have purchased **Dr.Web Anti-virus**.

After the key file is successfully checked, the updating is performed. The program automatically downloads all updated files, according to your version of **Dr.Web Anti-virus**, and, if your subscription terms allow, the new program version (if it is released).

The **Scanner** can use the updated databases after the next restart. **SpIDer Guard** and **SpIDer Mail** periodically check the state of the databases and start to use updated databases automatically.

When the **Updater** is launched from the **Scheduler** or in the command line mode, the command line parameters can be used (see Appendix A).

Appendices

Appendix A. Additional Command Line Parameters of the Anti-virus

Introduction

Additional command line parameters (switches) are used to set parameters for programs which can be launched by opening an executable file. This relates to scanners of all versions (read Using Dr.Web Scanner for Windows and Command Line Scanning Mode) and to the **Updater** (read Automatic Updating of the Virus Databases and Other Files of the Program). The switches can set the parameters unavailable in the configuration file and have a higher priority then the parameters which are specified in it.

Switches begin with the forward slash (**/**) character and are separated with blanks as other command line parameters.

The command line parameters for the scanner and for the automatic updating module are listed below. If a switch has modifications then they are specified as well.

The Scanner command line parameters

/? – display short help on the program and launch scanning.

/@<*file_name***>** or **/@+<***file_name***>** instructs to scan objects listed in the specified file. Each object is specified in a separate line of the list-file. It can be either a full path with the file name or the boot string which means that scanning of boot sectors should be performed. For the GUI-version of the scanner the file names with mask and directory names should be specified there. The list-file can be prepared manually in any text editor; it can also be made automatically by applications using the scanner to check certain files. After the scanning is made,

the scanner deletes the list-file, if used without the **+** character.

/AL – to scan all files in the given device, or in the given folder, regardless the extensions or the internal format.

/AR – to scan files inside the archives. At present, the scanning of archives (without curing) created by the ARJ, ZIP, PKZIP, ALZIP, RAR, LHA, GZIP, TAR, BZIP2, 7-ZIP, ACE, etc. archivers, as well as of MS CAB-archives – Windows Cabinet Files and ISO-images of optical disks (CD and DVD) is available. As it is specified (**/AR**) the switch instructs to inform a user if an archive with infected or suspicious files is detected. If the switch is supplemented with the **D**, **M** or **R** modifier, other actions are taken: **/ARD** – delete; **/ARM** – move (by default, to the infected.!!! directory); **/ARR** – rename (by default, the first character of extension is replaced by the # character). The switch may end with the **N** modifier, and in this case the name of the archiver after the name of the archived file will not be printed.

/CN – to set action for containers (HTML, RTF, PowerPoint) with infected or suspicious objects. As specified (**/CN**) the switch instructs to report such containers to a user. If **D**, **M** or **R** modifiers are added to the switch, a different action is applied: **/CND** – delete; **/CNM** – move (by default, to the infected.!!! directory); **/CNR** – rename (by default, the first character of extension is replaced by the # character). The switch may end with the **N** modifier, and in such case a message with the container type will not be printed.

/CU – actions with infected files and boot sectors of drives. The curable objects are cured and the incurable files are deleted without additional **D**, **M** or **R** modifiers (if different action is not specified by the **/IC** parameter). Other actions taken towards infected files: **/CUD** – delete; **/CUM** – move (by default, to the infected.!!! directory); **/CUR** – rename (by default, the first character of extension is replaced by the # character).

/DA – to scan the computer once a day. The next check date is logged into the configuration file and that is why it should be accessible for writing and subsequent rewriting.

/EX – to scan files with extensions listed in the configuration file by default, or, if unavailable, these are EXE, COM, DLL, SYS, VXD, OV?,

BAT, BIN, DRV, PRG, BOO, SCR, CMD, 386, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, PP?, OBJ, LIB, PIF, AR?, ZIP, R??, GZ, Z, TGZ, TAR, TAZ, CAB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SH, SHB, SHS, SHT*, MSG, CHM, XML, PRC, ASP, LSP, MSO, OBD, THE*, EML, NWS, SWF, MPP, TBB.

If an element of the list of scanned objects contains the explicit file extension, and it is used with special characters ***** and **?**, all files specified in this element of the list, and not only those matching this list of extensions, will be scanned.

/FAST perform an express scan of the system (for more information on the express scan mode see Launching the Scanner. General Information).

/FULL perform a full scan of all hard drives and removable data carriers (including boot sectors).

/GO – batch mode of the program. All questions implying answers from a user are skipped; solutions implying a choice are taken automatically. This mode is useful for automatic scanning of files, for example, during a daily (or weekly) check of the hard disk.

/HA – to perform heuristic scanning of files and search for unknown viruses in them.

/ICR, **/ICD** or **/ICM** – what to do with infected files which cannot be cured, **/ICR** – rename, **/ICD** – delete, **/ICM** – move.

/INI:<*path***>** – use alternative configuration file with specified name or path.

/LITE perform a basic scan of random access memory, boot sectors of all disks and startup objects.

/LNG:<*file_name***>** or **/LNG** – use alternative language resources file (DWL file) with specified name or path, and, if the path is not specified, – the inbuilt (English) language.

/ML – scan files of e-mail format (UUENCODE, XXENCODE, BINHEX

and MIME). As it is specified (**/ML**) the switch instructs to inform a user if an infected or suspicious object is detected in a mail archive. If the switch is supplemented with the **D**, **M** or **R** modifier, other actions are taken: **/MLD** – delete; **/MLM** – move (by default, to the infected.!!! directory); **/MLR** – rename (by default, the first character of extension is replaced by the # character). The switch may end with the N modifier. In this case the "Mail archive" message will not be displayed.

/MW – actions with all types of unsolicited programs. As it is specified (**/MW**) the switch instructs to inform a user. If the switch is supplemented with the **D**, **M**, **R** or **I** modifier, other actions are taken: **/MWD** – delete; **/MWM** – move (by default, to the infected.!!! directory); **/MWR** – rename (by default, the first character of extension is replaced by the # character); **/MWI** – ignore. Actions with some types of unsolicited programs are specified by the **/ADW**, **/DLS**, **/JOK**, **/RSK**, **/HCK** switches.

/NI – not to use parameters specified in **drweb32.ini** configuration file.

/NR – do not create a log file.

/NS – disable interrupting of a computer scanning. With this switch specified, a user will not be able to interrupt scanning by pressing [ESC].

/OK – display full list of scanned objects and mark the uninfected with **Ok**.

/PF – prompt on, if multiple floppies are scanned.

/PR – prompt for confirmation before action.

/QU – the scanner checks the objects specified in the command line (files, disks, directories) and then automatically terminates (for the GUI version of the scanner only).

/RP<*file_name***>** or **/RP+<***file_name***>** – log to a file the name of which is specified in the switch. If no name is specified, log to a default file. If the **+** character is present, the file is appended. If there

is no character, a new one is created.

/SCP:<*n*> – sets the priority of the scanning process, where <*n*> is a number ranging from 1 to 50.

/SD – scan subdirectories.

/SHELL – for the GUI version of the scanner. The switch disables the splash screen display, scanning of the memory and autorun files. This mode allows to use the GUI version of the scanner instead of the console version to scan only those objects which are listed in the command line parameters.

/SL – scan symbolic links (for **Console Scanner** only).

/SO – enables sounds.

/SPR, **/SPD** or **/SPM** – what to do with suspicious files, **/SPR** – rename, **/SPD** – delete, **/SPM** – move.

/SS – save the mode specified during the current program launch in the configuration file when the program terminates.

/ST – sets stealth mode of the GUI version of the scanner. The program operates without any windows opened and self-terminates. But, if during scanning virus objects were detected, the scanner window will be opened after the scanning made. Such scanner mode presupposes, that the list of the scanned objects is specified in the command line.

/TB – scan boot sectors and master boot records (MBR) of the hard drive.

/TM – search for viruses in main memory (including Windows system area, available for scanners for Windows only).

/TS – search for viruses in autorun files (in Autorun directory, system ini-files, Windows registry). It is used only in scanners for Windows.

/UPN – disable the output of names of file packers used for packing the scanned executable files to the log file.

/WA – do not terminate the program until any key is pressed, if viruses or suspicious objects are found (for console scanners only).

Certain parameters allow the "**-**" character to be used at the end. In such "negative" form the parameter means cancellation of the mode. Such option can be useful if this mode is enabled by default, or with the settings specified earlier in the configuration file. Here is the list of the command line parameters allowing "negative" form:

/ADW, **/AR**, **/CU**, **/DLS**, **/FAST**, **/FULL**, **/HA**, **/HCK**, **/IC**, **/JOK**, **/ML**, **/MW**, **/OK**, **/PF**, **/PR**, **/RSK**, **/SD**, **/SL**, **/SO**, **/SP**, **/SS**, **/TB**, **/TM**, **/TS**, **/WA**.

For **/CU**, **/IC** and **/SP** parameters the "negative" form cancels any actions specified in the description of these parameters. This means that infected and suspicious objects will be reported but no actions will be applied.

For **/INI** and **/RP** parameters the "negative" form is written as **/NI** and **/NR** accordingly.

For **/AL** and **/EX** the "negative" form is not allowed. However, specifying one of them cancels the other.

If several alternative parameters are found in the command line, the last of them takes effect.

For **/CU**, **/IC** and **/SP** parameters the "negative" form cancels any actions specified in the description of these parameters. This means that infected and suspicious objects will be reported but no actions will be applied.

For **/INI** and **/RP** parameters the "negative" form is written as **/NI** and **/NR** accordingly.

For **/AL** and **/EX** the "negative" form is not allowed. However, specifying one of them cancels the other.

If several alternative parameters are found in the command line, the last of them takes effect.

The DWScancl Console Scanner parameters

/AR – test archive files. Option is enabled by default.

/AC – test containers. Option is enabled by default.

/AFS – use forward slash to separate paths in archive. Option is disabled by default.

/ARC:<*ratio*> – maximum archive object compression. If the compression rate of the archive exceed the limit, **Console Scanner** neither unpacks, not scans the archive (*unlimited*).

/ARL:<*level*> – maximum archive level (*unlimited*).

/ARS:<*size*> – maximum archive size. if the archive size exceed the limit, **Scanner** neither unpacks, nor scans the archive (*unlimited*, KB).

/ART:<*size*> – minimim archive object matched by **/ARC**. minimum size of file inside archive beginning from which compression ratio check will be performed (*unlimited*, KB).

/ARX:<*size*> – maximum archive object size (*unlimited*, KB).

/BI – show virus bases info. Option is enabled by default.

/DR – recursive scan directory. Option is enabled by default.

/E:<*engines*> – maximum **Dr.Web** engines to use.

/FL:<*path*> – scan files listed in the specified file.

/FM:<*masks*> – scan files matched 'masks'. By default all files are scanned.

/FR:<*regexpr*> – scan files matched expression. By default all files are scanned.

/H or **/?** – show this message.

/HA – use heuristic analysis. Option is enabled by default.

/KEY:<*keyfile*> – use `keyfile' as activation key (by default drweb32.key or other suitable from C:\Program Files\DrWeb\).

/LN – resolve shell links. Option is disabled by default.

/LS – use LocalSystem account rights. Option is disabled by default.

/MA – test e-mail like files. Option is enabled by default.

/MC:<*limit*> – set maximum cure attempts number to 'limit' (*unlimited by default*).

/NB – don't backup curing/deleting files. Option is disabled by default.

/NI[:X] – nice mode 0-100, low resource usage (*unlimited*, %).

/NT – test NTFS streams. Option is enabled by default.

/OK – show OK for clean files. Option is disabled by default.

/P:<*prio*> – test priority:

0 – the lowest,
L – low,
N – general. Priority by default,
H – the highest,
M – maximal.

/PAL:<*level*> – maximum pack level. Value is 1000 by default.

/RA:<*file.log*> – add report into file.log. No report by default.

/RP:<*file.log*> – write report into file.log. No report by default.

/RPC:<*secs*> – **Dr.Web Scanning Engine** connection timeout. Timeout is 30 seconds by default.

/RPCD – use dynamic RPC identification.

/RPCE – use dynamic RPC endpoint.

/RPCE:<*name*> – use specified RPC endpoint.

/RPCH:<*name*> – use specified host name for remote call.

/RPCP:<*name*> – use specified RPC protocol. Possible protocols: lpc, np, tcp.

/QL – list quarantined files on all disks.

/QL:<*drive*> – list quarantined files on drive 'drive' (*letter*).

/QR[:[d][:p]] – delete quarantined files on drive 'd' (*letter*) older than 'p' days (*number*). Unspecified 'd' – all drives, unspecified 'p' – 0 days.

/QNA – double quote file names always.

/REP – go follow reparse points. Option is disabled by default.

/SCC – show content of compound objects. Option is disabled by default.

/SCN – show container name. Option is disabled by default.

/SPN – show packer name. Option is disabled by default.

/SLS – show log on screen. Option is enabled by default.

/SPS – show progress on screen. Option is enabled by default.

/SST – show file scan time. Option is disabled by default.

/TB – test boot sectors. Option is disabled by default.

/TM – test processes in memory. Option is disabled by default.

/TS – test system startup processes. Option is disabled by default.

/TR – test system restore points directories. Option is disabled by

default.

/W:<*sec*> – maximum time to scan (*unlimited*, sec).

/WCL – drwebwcl compatible output.

/X:S[:R] – set power state shutDown/Reboot/Suspend/Hibernate with reason '**R**' (for shutdown/reboot).

Action for different objects (**C** - cure, **Q** - move to quarantine, **D** - delete, **I** - ignore, **R** - inform. **R** is set by default for all objects):

/AAD:X – action for adware (**R**, possible DQIR).

/AAR:X – action for infected archive files (**R**, possible DQIR).

/ACN:X – action for infected container files (**R**, possible DQIR).

/ADL:X – action for dialers (**R**, possible DQIR).

/AHT:X – action for hacktools (**R**, possible DQIR).

/AIC:X – action for incurable files (**R**, possible DQR).

/AIN:X – action for infected files (**R**, possible CDQR).

/AJK:X – action for jokes (**R**, possible DQIR).

/AML:X – action for infected e-mail files (**R**, possible QIR).

/ARW:X – action for riskware (**R**, possible DQIR).

/ASU:X – action for suspicious files (**R**, possible DQIR).

Several parameters can have modifiers that clearly enable or disable options specified by these keys. For example:

/AC- option is clearly disabled,
/AC, **/AC+** option is clearly enabled.

These modifiers can be useful if option was enabled or disabled by default or was set in configuration file earlier. Keys with modifiers are listed below:

/AR, **/AC**, **/AFS**, **/BI**, **/DR**, **/HA**, **/LN**, **/LS**, **/MA**, **/NB**, **/NT**, **/OK**, **/QNA**, **/REP**, **/SCC**, **/SCN**, **/SPN**, **/SLS**, **/SPS**, **/SST**, **/TB**, **/TM**, **/TS**, **/TR**, **/WCL**.

For **/FL** parameter "**-**" modifier directs to scan paths listed in specified file and then delete this file.

For **/ARC**, **/ARL**, **/ARS**, **/ART**, **/ARX**, **/NI[:X]**, **/PAL**, **/RPC** and **/W** parameters "0" value means that there is no limit.

Example of using command line parameters with **DWScancl Console Scanner**:

[<*path_to_file*>]`dwscancl /AR- /AIN:C /AIC:Q C:\`

scan all files on disk C:, excluding those in archives; cure the infected files and move to quarantine those that cannot be cured.

Automatic Updating Module command line parameters

If the **Updater** is run automatically or in the command line mode, you can input the following command line parameters:

/DBG – detailed log.

The modes, specified by default (if no configuration file is available or used) are described in the table in Appendix B. Adjustable parameters of Dr.Web components.

/DIR:<*directory***>** – change of the name of the folder where the updated files are placed; by default, the folder from which the **Updater** was launched is used.

/INI:<*path***>** – use alternative configuration file with specified name or path.

/GO – package operation mode, without dialogs.

/LNG:<*file_name***>** – language resources file name; if not specified, English is used.

/NI – do not use parameters specified in drweb32.ini configuration file.

/NR – do not create a log file.

/PASS:<*user password of http-server***>** – user password of the updating server.

/PPASS:<*proxy user password***>** – user password for the proxy server.

/PUSER:<*proxy user name***>** – user name for the proxy server.

/PURL:<*proxy address***>** – address of a proxy server.

/QU – to compulsory close the automatic utility after the updating is finished, regardless whether it was successful or not. The success of the updating can be checked via the drwebupw.exe return code (for example, from the bat-file by the errorlevel variable value: 0 – successful, other values – unsuccessful).

/REG – launch of the updating module for registration and receipt of a registration key file.

/RP<*file_name***>** or **/RP+<***file_name***>** – log to a file the name of which is specified in the switch. If no name is specified, log to a file with the default name. If the + character is present, the file is appended, if there is no character, a new one is created.

/SETTINGS – display the **Updater** settings.

/SO – enables sounds (only when errors occur).

/ST – run the automatic utility in invisible mode (stealth mode).

/UA – download all files specified in the updating list, regardless the

used operating system and the installed components. The mode is designed for receipt of the full local copy of the **Dr.Web** server updating area; this mode cannot be used for updating the anti-virus installed on a computer.

/UPD – usual updating; it is used together with the /REG: switch - to run the updating session itself during the registration.

/UPM:<*proxy mode***>** – mode of using a proxy server, it can have the following values:

- **direct** – do not use proxy server
- **ieproxy** – use system settings
- **userproxy** – use settings specified by a user (in the **Update** pane of the **Dr.Web** toolbar or by the /PURL /PUSER /PPASS)

/URL:<*url of the updating server***>** – only UNC-paths are accepted.

/URM:<*mode***>** – to restart after the updating is finished. It can have the following values:

- **prompt** – prompt if a reboot is needed after the updating session is finished
- **noprompt** – if necessary, reboot without prompting
- **force** – reboot always (regardless whether it is required for the updating or not)
- **disable** – disable reboot

/USER:<*user name of http-server***>** – user name for the updating server.

/UVB – update the virus databases and drweb32.dll kernel only (disables **/UA**, if it is set).

/SO parameter allows the "**-**" character at the end. In such "negative" form the parameter means cancellation of the mode. This option can be useful if the mode is enabled with the settings specified earlier in the configuration file.

For **/INI** and **/RP** parameters the "negative" form is written as **/NI**

and **/NR** accordingly.

If several alternative parameters are found in the command line, the last of them takes effect.

Return codes

The values of the return code and corresponding events are as follows:

Return code value	Event
0	OK, no virus found
1	known virus detected
2	modification of known virus detected
4	suspicious object found
8	known virus detected in file archive, mail archive or container
16	modification of known virus detected in file archive, mail archive or container
32	suspicious file found in file archive, mail archive or container
64	at least one infected object successfully cured
128	at least one infected or suspicious file deleted/ renamed/moved

The actual value returned by the program is equal to the sum of codes for the events that occurred during scanning. Obviously, the sum can be easily decomposed into separate event codes.

For example, return code 9 = 1 + 8 means that known viruses were detected, including viruses in archives, mail archives or containers; curing and others actions were not executed; no other "virus" events occurred during scanning.

Appendix B. Adjustable Parameters of Dr.Web Components

Introduction

Adjustable parameters of the program components (except **SpIDer Guard**) are stored mainly in the program's configuration file (drweb32.ini resides in the installation folder). This is a text file and has separate sections for different components. Each parameter of any component is specified in the correspondent section as a string `parameter = value`.

The values of parameters can be changed in one of the following ways:

- via the interface of the corresponding program (**Scanner**, **SpIDer Mail**). The most important of such settings are described above (read Adjusting the Scanner Settings, Adjusting Certain Program Settings);
- by setting command line parameters when calling programs from the command line or according to schedule (for the **Scanner** of different versions). Read Appendix A for more details on this option;
- by editing the configuration file via any text editor.

Only experienced users should edit the configuration file. Using this option without clear understanding of the anti-virus structure may degrade the reliability of the anti-virus protection or even result in failure of some programs.

The parameters of the Windows versions of the Scanner and Updater

The following data for every parameter is displayed in columns of the table:

- parameter name
- name of components using the parameter
- parameter name in the configuration file
- parameter values
- command line keys

The parameter name is either printed in conformity with the interface (printed in bold), or as a conventional name, if no parameter in the interface corresponds to it (printed in light type).

In the Table "Scanner" is used for both versions of the **Scanner** ("Scanner-GUI" and "Console scanner").

If a correspondent parameter of the configuration file is missing for some mode, the values of parameters are specified in brackets and relate to the interface dialog element or to the specified command line switch.

The command line switches corresponding to the given parameter are described shortly, without the majority of modifiers. Detailed information on switches is given in Appendix A.

Parameter	Components	Configur. file parameter	Values	Keys
Scan mode	Scanner	ScanFiles	All ByType ByMasks	/AL /EX
Express scan of the system	Scanner			/FAST
Full scan of the system	Scanner			/FULL

Parameter	Components	Configur. file parameter	Values	Keys
Priority of the scanning process, from 1 to 50	Scanner			/SCP
Heuristic analysis	Scanner	HeuristicAnalysis	Yes / No	/HA
Scan memory	Scanner	TestMemory	Yes / No	/TM
Scan autorun files	Scanner	TestStartup	Yes / No	/TS
Scan boot sectors	Scanner	TestBootSectors	Yes / No	/TB
Scan subfolders	Scanner	ScanSub Directories	Yes / No	/SD
Prompt on multiple floppies	Scanner	PromptFloppy	Yes / No	/PF
Archives	Scanner	CheckArchives	Yes / No	/AR
Mail files	Scanner	CheckEMailFiles	Yes / No	/ML
Max size of unpacked archive to check, KB	Console Scanner	MaxFileSizeTo Extract	(empty)	
Max compression ratio for archive	Console Scanner	MaxCompressio nRatio	(empty)	
Threshold for MaxCompressio nRatio, KB	Console scanner	Compression CheckThreshold	(empty)	
List of extensions	Scanner	FilesTypes	(see below the Table)	

Parameter	Components	Configur. file parameter	Values	Keys
List of masks	Scanner	UserMasks	(see below the Table)	
Locations of excluded folders	Scanner	ExcludePaths	(empty)	
Excluded files	Scanner	ExcludeFiles	(empty)	
Scan hard drives (if scanned with the * command line parameter and when the Select drives button is pressed)	Scanner	ScanHDD	Yes / No	
Scan floppies (if scanned with the * command line parameter and when the Select drives button is pressed)	Scanner	ScanFDD	Yes / No	
Scan compact disks (if scanned with the * command line parameter and when the Select drives button is pressed)	Scanner	ScanCD	Yes / No	

Parameter	Components	Configur. file parameter	Values	Keys
Scan network disks (if scanned with the * command line parameter and when the Select drives button is pressed)	Scanner	ScanNet	Yes / No	
Prompt on action	Scanner	PromptOnAction	Yes / No	/PR
Rename extension	Scanner	RenameFilesTo	#??	
Move path	Scanner	MoveFilesTo	infected.!!!	
Location of virus databases	Scanner	VirusBase	*.vdb	
Path to the folder with temporary files of the component	Scanner	TempPath	%TMP%, %TEMP%, install directory	
Actions with all types of malicious programs	Scanner		Report	/MW
Infected objects	Scanner	InfectedFiles	Report Cure Delete Rename Move Lock (guard) Shutdown (guard)	/CU

Parameter	Components	Configur. file parameter	Values	Keys
Incurable objects	Scanner	IncurableFiles	Report Delete Rename Move Lock (guard) Shutdown (guard)	/IC
Suspicious objects	Scanner	SuspiciousFiles	Report Delete Rename Move Lock (guard) Ignore (guard) Shutdown (guard)	/SP
Infected archives	Scanner	ActionInfected Archive	Report Delete Rename Move Lock (guard) Ignore (guard) Shutdown (guard)	/AR
Infected mail files	Scanner	ActionInfected Mail	Report Delete Rename Move Lock (guard) Ignore (guard) Shutdown (guard)	/ML

Parameter	Components	Configur. file parameter	Values	Keys
Adware programs	Scanner	ActionAdware	Report Delete Rename Move Ignore Lock (guard) Shutdown (guard)	/ADW
Dialer programs	Scanner	ActionDialers	Report Delete Rename Move Ignore Lock (guard) Shutdown (guard)	/DLS
Joke programs	Scanner	ActionJokes	Report Delete Rename Move Ignore Lock (guard) Shutdown (guard)	/JOK
Riskware	Scanner	ActionRiskware	Report Delete Rename Move Ignore Lock (guard) Shutdown (guard)	/RSK

Parameter	Components	Configur. file parameter	Values	Keys
Hacktools	Scanner	ActionHacktools	Report Delete Rename Move Ignore Lock (guard) Shutdown (guard)	/HCK
Permit archives deletion without a prompt	Scanner	EnableDelete ArchiveAction	Yes / No	
Log to file	Scanner, Updating module	LogToFile	Yes / No	/RP /NR
Log file name	Scanner	LogFileName	drweb32 w.log spiderg3. log	/RP
Log file name	Updating module		drwebup w.log	/RP
Log mode	Scanner, Updating module	OverwriteLog	Yes / No	/RP
Log encoding	Scanner, Updating module	LogFormat	ANSI OEM	
Scanned objects in log file	Scanner	LogScanned	Yes / No	/OK
Names of file packers in log file	Scanner	LogPacked	Yes / No	

Parameter	Components	Configur. file parameter	Values	Keys
Names of archivers in report	Scanner	LogArchived	Yes / No	
Statistics in log file	Scanner	LogStatistics	Yes / No	
Maximum log file size	Scanner, Updating module	LimitLog	Yes / No	
Log size limit, KB	Scanner, Updating module	MaxLogSize	512 8192	
Close the window after sessions	Scanner, Updating module		Yes / No	/QU
Wait for a key to be pressed as soon as scanning is complete (in case a virus is detected)	Console scanner	WaitAfterScan	(On / Off)	/WA
Operate in packet mode	Scanner, Updating module		(On / Off)	/GO
Prohibit interruption by a user	Scanner		(On / Off)	/NS
Scan once a day	Scanner		(On / Off)	/DA
Scan the explicitly selected objects only	Scanner-GUI		(On / Off)	/ SHELL

Parameter	Components	Configur. file parameter	Values	Keys
Do not open windows (stealth mode)	Scanner-GUI		(On / Off)	/ST
Use alternative configuration file. Do not use any configuration file	Scanner, Updating module		(On / Off)	/INI /NI
Use own swap file	Scanner	UseDiskForSwap	Yes / No	
Display progress bar	Scanner	ShowProgress Bar	Yes / No	
Sounds	Scanner, Updating module	PlaySounds	Yes / No	/SO
Alert (sound)	Scanner	AlertWav	alert.wav	
Cured (sound)	Scanner	CuredWav	cured. wav	
Deleted (sound)	Scanner	DeletedWav	deleted. wav	
Renamed (sound)	Scanner	RenamedWav	renamed. wav	
Moved (sound)	Scanner	MovedWav	moved. wav	
Finish (sound)	Scanner	FinishWav	finish.wav	
Error (sound)	Scanner, Updating module	ErrorWav	error.wav	
Autosave settings	Scanner	AutoSave Settings	Yes / No	/SS

Parameter	Components	Configur. file parameter	Values	Keys
Use registry settings	Scanner-GUI		(On / Off)	
Scan priority	Scanner	ScanPriority	25 50	
Language	Scanner, Updating module	LngFileName	ru-drweb.dwl	/LNG
Proxy mode	Scanner-GUI (the updating module settings)	UpdateProxyMode	direct ieproxy userproxy	/UPM
Update the virus databases and drweb32.dll kernel only	Updating module	UpdateVirusBasesOnly	Yes / No	/UVB
Download all files from the update list	Updating module	UpdateAllFiles	Yes / No	/UA
Reboot mode at updating	Updating module	UpdateRebootMode	prompt noprompt force disable	/URM
Log details	Updating module		(On / Off)	/DBG

By default, the list of file extensions (the **FilesTypes** parameter value) contains the following extensions: EXE, COM, DLL, SYS, VXD, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, 386, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, PP?, OBJ, LIB, PIF, AR?, ZIP, R??, GZ, Z, TGZ, TAR, TAZ, CAB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SH, SHB, SHS, SHT*, MSG, CHM, XML, PRC, ASP, LSP, MSO, OBD, THE*, EML, NWS, SWF, MPP, TBB.

By default, the list of selected masks (the **UserMasks** parameter value of the configuration file) contains the values formed by adding

the asterisk * symbol and a full stop before an extension from the list of file extensions (for example, ***.exe**).

Parameters of SpIDer Mail

Parameters of **SpIDer Mail** are described in the table below. The layout of this table is similar to that of the table above. In the list of admissible parameter values, the default values for **SpIDer Mail** are given in italics.

Parameter	Configuration file parameter	Value	Key
Use alternative configuration file		(On / Off)	-ini: file_name
Use alternative user key file		(On / Off)	-key: file_name
Language	LngFileName	ru-drweb.dwl	-lng: file_name
Heuristic analysis	HeuristicAnalysis	Yes / No	
Check archive files	CheckArchives	Yes / No	
Virus activity control	VirusActivityControl	Yes / No	
Message scan timeout, s	ScanTimeout	250	
Max file size to extract, KB	MaxFileSizeToExtract	30720	
Max compression ratio	MaxCompressionRatio	Infinite	
Max archive level	MaxArchiveLevel	64	
Show virus alerts for outgoing mail	ShowAlerts	Yes / No	
Infected messages	ActionInfected	Delete Move	
Suspicious messages	ActionSuspicious	Delete Move Skip	

Parameter	Configuration file parameter	Value	Key
Not checked messages	ActionNotChecked	Delete Move Skip	
Delete modified messages on the server	DeleteMessagesOnServer	Yes / No	
Insert 'X-AntiVirus' header into messages	InsertXAntiVirus	Yes / No	
Path to quarantine	PathForMovedFiles	infected.!!!	
Path to Dr.Web engine	EnginePath	(empty)	
Path to Dr.Web virus database	VirusBasesPath	(empty)	
Flag file to detection update	UpdateFlag	drwtoday.vdb	
Period to check flag file, s	UpdatePeriod	300	
Maximum load engines	MaximumLoadEngines	10	
Preload engines	PreloadEngines	1	
Unused engine unload timeout, s	UnusedEngineUnloadTimeout	420	
Enable logging	EnableLog	Yes / No	
Enable logging scan info	EnableLogScanInfo	Yes / No	
Log to file	LogFileName	spiderml.log	
Maximum log file size, KB	MaximumLogSize	500	

Parameter	Configuration file parameter	Value	Key
Enable icon animation	EnableIconAnimation	Yes / No	
Enable tray icon	HideIcon	Yes / No	
Show notifications	NoBalloons	Yes / No	
Intercept connections automatically or Manual connections setup radio buttons	HookModeAuto	Yes / No	
Test interception functionality on every starting (aut.mode)	HookCheck	Yes / No	
Address-Port (the first element of the list, aut.mode)	Hook1	*:143 address: port	
Address-Port (continuation of the list, aut.mode)	Hook2 Hook3 …	address: port address: port …	
SpIDerMail port-Server address – Server port (manual mode, first element of the list)	HookManual1	7000 -> address POP3/ SMTP/ IMAP4/ NNTP: port	

Parameter	Configuration file parameter	Value	Key
SpIDerMail port-Server Address - Server Port (manual mode, continuation of the list)	HookManual2 HookManual3 …	7001 -> address POP3/ SMTP/ IMAP4/ NNTP: port 7002 -> address POP3/ SMTP/ IMAP4/ NNTP: port …	
Enable the Disable menu item	AllowDisable	Yes / No	
Enable the Exit menu item	AllowExit	Yes / No	
Enable the Settings menu item	AllowSettings	Yes / No	
Enable the Reinitialize menu item	AllowReinitialize	Yes / No	
Max simultaneously processed queries at one local port (manual mode)	MaximumChildConnections	20	
A string added to message	Xbanner	(empty)	
Path to temporary files directory of the component	TempPath	%TMP%, %TEMP%, install directory	

Parameter	Configuration file parameter	Value	Key
Reinitialize			-reinit
Disable			-disable
Enable			-enable
Update			-update
Exit			-exit

Appendix C. Malicious Programs and Methods of Neutralizing Them

With the development of computer technologies and network solutions malicious programs (malware) of different kinds, meant to strafe users, become more and more widespread. Their development began together with computer science and facilities of protection against them progressed alongside. Nevertheless, there is still no common classification for all possible threats due to their unpredictable development character and constant improvement of applicable technologies.

Malicious programs can be distributed through the Internet, local area networks, e-mail and portable data mediums. Some of them rely on the user's carelessness and lack of experience and can be run in completely automatic mode. Others are tools controlled by a computer cracker and they can harm even the most secure systems.

This chapter describes all of the most common and widespread types of malware, against which products of **Doctor Web, Ltd.** are aimed.

Classification of malicious programs and other computer threats

Computer viruses

This type of malicious programs is characterized by the ability to implement its code into the executable code of other programs. Such implementation is called infection. In most cases the infected file becomes a virus carrier itself and the implemented code does not necessarily match the original. Most viruses are intended to damage or destroy data on the system. Viruses which infect files of the operating system (usually executable files and dynamic libraries) and activate upon launching of the infected file are called file viruses.

Some viruses infect boot records of diskettes and partitions or master boot records of fixed disks. Such viruses are called boot viruses. They

take very little memory and remain ready to continue performing their tasks until a system roll-out, restart or shut-down occurs.

Macroviruses are viruses which infect documents used by the Microsoft Office and some other applications which allow macro commands (usually written in Visual Basic). Macro commands are a type of implemented programs (macros) written in a fully functional programming language. For instance, in Microsoft Word macros can automatically initiate upon opening (closing, saving, etc.) a document.

A virus which has the ability to activate and perform the tasks assigned by the virus writer only when the computer reaches a certain state (e. g. a certain date and time) is called a memory-resident virus.

Most viruses have some kind of protection against detection. Protection methods are being constantly improved and ways to overcome them are developed.

Encrypted viruses, for instance, cipher their code upon every infection to hamper their detection in a file, boot sector or memory. All copies of such viruses contain only a small common code fragment (the decryption procedure), which can be used as a virus signature.

Polymorphic viruses also encrypt there code, but besides that they generate a special decryption procedure which is different in every copy of the virus. This means that such viruses do not have byte signatures.

Stealth viruses perform certain actions to disguise their activity and thus conceal their presence in an infected object. Such viruses gather the characteristics of a program before infecting it and then plant these "dummy" characteristics which mislead the scanner searching for modified files.

Viruses can also be classified according to the programming language in which they are written (in most cases it is assembler, high-level programming languages, scripting languages, etc.) or according to the affected operating systems.

Computer worms

Worms have become a lot more widespread than viruses and other malicious programs recently. Like viruses they are able to reproduce themselves and spread their copies but they do not infect other programs. A worm infiltrates the computer from the worldwide or local network (usually via an attachment to an e-mail) and distributes its functional copies to other computers in the network. It can begin distributing itself either upon a user's action or in an automatic mode, choosing which computers to attack.

Worms do not necessarily consist of only one file (the worm's body). Many of them have an infectious part (the shellcode), which loads into the main memory (RAM) and then downloads the worm's body as an executable file via the network. If only the shellcode is present in the system, the worm can be rid of by simply restarting the system (at which the RAM is erased and reset). However, if the worm's body infiltrates the computer, then only an anti-virus program can cope with it.

Worms have the ability to cripple entire networks even if they do not bear any payload (i.e. do not cause any direct damage) due to their intensive distribution.

Trojan horses (Trojans)

This type of malicious program cannot reproduce or infect other programs. A Trojan substitutes a high-usage program and performs its functions (or imitates the programs operation). At the same time it performs some malicious actions in the system (damages or deletes data, sends confidential information, etc.) or makes it possible for another person to access the computer without permission, e.g. to harm the computer of a third party.

A Trojan's masking and malicious facilities are similar to those of a virus and it can even be a component of a virus. However, most Trojans are distributed as separate executable files (through file-exchange servers, removable data carriers or e-mail attachments), which are launched by a user or a system task.

Rootkits

It is a type of malicious program used to intercept system functions of an operating system in order to conceal itself. Besides, a rootkit can conceal tasks of other programs, registry keys, folders and files. It can be distributed either as an independent program or a component of another malicious program. A rootkit is basically a set of utilities, which a cracker installs on a system to which she had just gained access.

There are two kinds of rootkits according to the mode of operation: User Mode Rootkits (UMR) which operate in user mode (intercept functions of the user mode libraries) and Kernel Mode Rootkits (KMR) which operate in kernel mode (intercept functions on the level of the system kernel, which makes it harder to detect).

Hacktools

Hacktools are programs designed to assist the intruder with hacking. The most common among them are port scanners which detect vulnerabilities in firewalls and other components of the computer's protection system. Besides hackers, such tools are used by administrators to check the security of their networks. Occasionally, common software which can be used for hacking and various programs that use social engineering techniques are designated as among hacktools as well.

Spyware

This type of malicious programs is designed to perform monitoring of the system and send the gathered information to a third party – creator of the program or some other person concerned. Among those who may be concerned are: distributors of spam and advertisements, scam-agencies, marketing agencies, criminal organizations, industrial espionage agents, etc.

Spyware is secretly loaded to your system together with some other software or when browsing certain HTML-pages and advertising windows. It then installs itself without the user's permission. Unstable browser operation and decrease in system performance are common side effects of spyware presence.

Adware

Usually this term is referred to a program code implemented into freeware programs which perform forced display of advertisements to a user. However, sometimes such codes can be distributed via other malicious programs and show advertisements in internet-browsers. Many adware programs operate with data collected by spyware.

Joke programs

Like adware, this type of malicious programs does not deal any direct damage to the system. Joke programs usually just generate message boxes about errors that never occurred and threaten to perform actions which will lead to data loss. Their purpose is to frighten or annoy a user.

Dialers

These are special programs which are designed to scan a range of telephone numbers and find those where a modem answers. These numbers are then used to mark up the price of telephoning facilities or to connect the user to expensive telephone services.

All the above programs are considered malicious because they pose a threat to the user's data or his right of confidentiality. Programs that do not conceal their presence, distribute spam and different traffic analyzers are usually not considered malicious, although they can become a threat under certain circumstances.

Among other programs there is also a class of riskware programs. These were not intended as malicious, but can potentially be a threat to the system's security due to their certain features. Riskware programs are not only those which can accidentally damage or delete data, but also ones which can be used by crackers or some malicious programs to do harm to the system. Among such programs are various remote chat and administrative tools, FTP-servers, etc.

Below is a list of various hacker attacks and internet fraud:

- **Brute force attack** – performed by a special Trojan horse program, which uses its inbuilt password dictionary or generates random symbol strings in order to figure out the network access password by trial-and-error.
- **DoS-attack** (denial of service) or **DDoS-attack** (distributed denial of service) – a type of network attack, which verges on terrorism. It is carried out via a huge number of service requests sent to a server. When a certain number of requests is received (depending on the server's hardware capabilities) the server becomes unable to cope with them and a denial of service occurs. DDoS-attacks are carried out from many different IP-addresses at the same time, unlike DoS-attacks, when requests are sent from one IP-address.
- **Mail bombs** – a simple network attack, when a big e-mail (or thousands of small ones) is sent to a computer or a company's mail server, which leads to a system breakdown. There is a special method of protection against such attacks used in the Dr. Web products for mail servers.
- **Sniffing** – a type of network attack also called "passive tapping of network". It is unauthorized monitoring of data and traffic flow performed by a packet sniffer – a special type of non-malicious program, which intercepts all the network packets of the monitored domain.
- **Spoofing** – a type of network attack, when access to the network is gained by fraudulent imitation of connection.
- **Phishing** – an Internet-fraud technique, which is used for stealing personal confidential data such as access passwords, bank and identification cards data, etc. Fictitious letters supposedly from legitimate organizations are sent to potential victims via spam mailing or mail worms. In these letters victims are offered to visit phony web sites of such organizations and confirm the passwords, PIN-codes and other personal information, which is then used for stealing money from the victim's account and for other crimes.
- **Vishing** – a type of Phishing technique, in which war dialers or VoIP is used instead of e-mails.

Actions applied to malicious programs

There are many methods of neutralizing computer threats. Products of **Doctor Web, Ltd.** combine these methods for the most reliable protection of computers and networks using flexible user-friendly settings and a comprehensive approach to security assurance. The main actions for neutralizing malicious programs are:

Cure – an action applied to viruses, worms and trojans. It implies deletion of malicious code from infected files or deletion of a malicious program's functional copies as well as the recovery of affected objects (i.e. return of the object's structure and operability to the state which was before the infection) if it is possible. Not all malicious programs can be cured. However, products of **Doctor Web, Ltd.** are based on more effective curing and file recovery algorithms compared to other anti-virus manufacturers.

Move to quarantine – an action when the malicious object is moved to a special folder and isolated from the rest of the system. This action is preferable in cases when curing is impossible and for all suspicious objects. It is recommended to send copies of such files to the virus laboratory of **Doctor Web, Ltd.** for analysis.

Delete – the most effective action for neutralizing computer threats. It can be applied to any type of malicious objects. Note, that deletion will sometimes be applied to certain files for which curing was selected. This will happen if the file contains only malicious code and no useful information. E.g. curing of a computer worm implies deletion of all its functional copies.

Block, rename – these actions can also be used for neutralizing malicious programs. However, fully operable copies of these programs remain in the file system. In case of the Block action all access attempts to or from the file are blocked. The Rename action means that the extension of the file is renamed which makes it inoperative.

Appendix D. Naming of Viruses

Specialists of the **Dr.Web Virus Laboratory** give names to all collected samples of computer threats. These names are formed according to certain principles and reflect a threat's design, classes of vulnerable objects, distribution environment (OS and applications) and some other features. Knowing these principles may be useful for understanding software and organizational vulnerabilities of the protected system. In certain cases this classification is conventional, as some viruses can possess several features at the same time. Besides, it should not be considered exhaustive, as new types of viruses constantly appear and the classification is made more precise. The full and constantly updated version of this classification is available at the Dr.Web web site.

The full name of a virus consists of several elements, separated with full stops. Some elements at the beginning of the full name (prefixes) and at the end of it (suffixes) are standard for the accepted classification. Below is a list of all prefixes and suffixes used in **Dr.Web** divided into groups.

Prefixes

Affected operating systems

The prefixes listed below are used for naming viruses infecting executable files of certain OS's:

- Win – 16-bit Windows 3.1 programs
- Win95 – 32-bit Windows 95/98/Me programs
- WinNT – 32-bit Windows NT/2000/XP/Vista programs
- Win32 – 32-bit Windows 95/98/Me and NT/2000/XP/Vista programs
- Win32.NET – programs in Microsoft .NET Framework operating system
- OS2 – OS/2 programs

- Unix – programs in various Unix-based systems
- Linux – Linux programs
- FreeBSD – FreeBSD programs
- SunOS – SunOS (Solaris) programs
- Symbian – Symbian OS (mobile OS) programs

Note that some viruses can infect programs of one system even if they are designed to operate in another system.

Macrovirus prefixes

The list of prefixes for viruses which infect MS Office objects (the language of the macros infected by such type of virus is specified):

- WM – Word Basic (MS Word 6.0-7.0)
- XM – VBA3 (MS Excel 5.0-7.0)
- W97M – VBA5 (MS Word 8.0), VBA6 (MS Word 9.0)
- X97M – VBA5 (MS Excel 8.0), VBA6 (MS Excel 9.0)
- A97M – databases of MS Access'97/2000
- PP97M – MS PowerPoint presentations
- O97M – VBA5 (MS Office'97), VBA6 (MS Office 2000); this virus infects files of more than one component of MS Office

Development languages

The HLL group is used to name viruses written in high level programming languages, such as C, C++, Pascal, Basic and others.

- HLLW – worms
- HLLM – mail worms
- HLLO – viruses overwriting the code of the victim program,
- HLLP – parasitic viruses
- HLLC – companion viruses

The following prefix also refers to development language:

- Java – viruses designed for the Java virtual machine

Script-viruses

Prefixes of viruses written in different scrip languages:

- VBS – Visual Basic Script
- JS – Java Script
- Wscript – Visual Basic Script and/or Java Script
- Perl – Perl
- PHP – PHP
- BAT – MS-DOS command interpreter

Trojan horses

- Trojan – a general name for different Trojan horses (Trojans). In many cases the prefixes of this group are used with the Trojan prefix.
- PWS – password stealing Trojan
- Backdoor – Trojan with RAT-function (Remote Administration Tool – a utility for remote administration)
- IRC – Trojan which uses Internet Relay Chat channels
- DownLoader – Trojan which secretly downloads different malicious programs from the Internet
- MulDrop – Trojan which secretly downloads different viruses contained in its body
- Proxy – Trojan which allows a third party user to work anonymously in the Internet via the infected computer
- StartPage (synonym: Seeker) – Trojan which makes unauthorized replacement of the browser's home page address (start page)
- Click – Trojan which redirects a user's browser to a certain web site (or sites)
- KeyLogger – a spyware Trojan which logs key strokes; it may send collected data to a malefactor
- AVKill – terminates or deletes anti-virus programs, firewalls, etc.
- KillFiles, KillDisk, DiskEraser – deletes certain files (all files on drives, files in certain directories, files by certain mask, etc.)
- DelWin – deletes files vital for the operation of Windows OS

- FormatC – formats drive C
- FormatAll – formats all drives
- KillMBR – corrupts or deletes master boot records (MBR)
- KillCMOS – corrupts or deletes CMOS memory

Tools for network attacks

- Nuke – tools for attacking certain known vulnerabilities of operating systems leading to abnormal shutdowns of the attacked system
- DDoS – agent program for performing a DDoS-attack (Distributed Denial Of Service)
- FDoS (synonym: Flooder) – programs for performing malicious actions in the Internet which use the idea of DDoS-attacks; in contrast to DDoS, when several agents on different computers are used simultaneously to attack one victim system, an FDoS-program operates as an independent "self-sufficient" program (Flooder Denial of Service)

Malicious programs

- Adware – an advertising program
- Dialer – a dialer program (redirecting modem calls to predefined paid numbers or paid resources)
- Joke – a joke program
- Program – a potentially dangerous program (riskware)
- Tool – a program used for hacking (hacktool)

Miscellaneous

- Exploit – a tool exploiting known vulnerabilities of an O S or application to implant malicious code or perform unauthorized actions.
- Generic – this prefix is used after another prefix describing the environment or the development method to name a typical representative of this type of viruses. Such virus does not possess any characteristic features (such as text strings, special effects, etc.) which could be used to assign it some specific name.

- Silly – this prefix was used to name simple featureless viruses the with different modifiers in the past.

Suffixes

Suffixes are used to name some specific virus objects:

- Origin – this suffix is added to names of objects detected using the *Origins Tracing* algorithm.
- generator – an object which is not a virus, but a virus generator.
- based – a virus which is developed with the help of the specified generator or a modified virus. In both cases the names of this type are generic and can define hundreds and sometimes even thousands of viruses.
- dropper – an object which is not a virus, but an installer of the given virus.

Appendix E. Corporate network protection by Dr.Web® Enterprise Suite

Dr.Web provides reliable, flexible and easy customized protection against viruses and other unsolicited programs.

The versions of the program designed for Windows, as well as versions for other platforms, provide reliable computer protection in a company. Still, the functioning of computers within a corporate network has certain problems for the anti-virus protection:

- usually, the software is installed onto computers by a company network administrator. The installation of anti-virus programs, their timely updating is an additional work for the administrator and requires physical access to computers;
- any changes made in the settings of the anti-virus by an inexperienced user (including its disabling because of the seeming inconveniences) generate "holes" in protection – the viruses begin to penetrate inside the corporate network and their disinfection becomes a much more complicated task;
- the anti-virus protection can be fully efficient if its operation is analyzed by qualified specialists which includes analysis of protocols, files moved to the quarantine, etc. This work may be difficult in conditions, when this data is kept in dozens or hundreds computers.

To solve these problems, **Dr.Web Enterprise Suite** (**Dr.Web ES**) was developed.

Dr.Web Enterprise provides for:

- centralized (without user intervention) installation of the anti-virus packages on computers,
- centralized setup of the anti-virus packages,
- centralized virus databases and program files updates on protected computers,
- monitoring of virus events and the state of the anti-virus packages and OS's on all protected computers.

Dr.Web ES allows both to grant the users of the protected computers with the permissions to set up and administer the anti-virus packages on their computers, or flexibly limit their rights, including absolute prohibition.

Dr.Web ES has a *client-server* architecture. **Dr.Web ES** components are installed on the computers of users and administrators and the computer(s) to function as the **Enterprise Server(s)**, and exchange information through network protocols TCP/IP, IPX/SPX, NetBIOS. An aggregate of computers on which **Dr.Web ES** cooperating components are installed is called an *anti-virus network*.

An anti-virus network includes the following components:

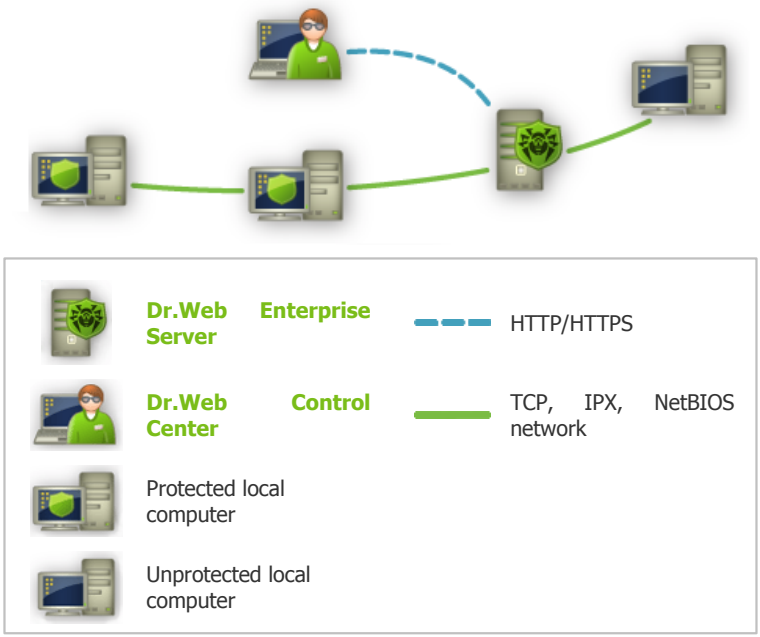
Core components:

- *Dr.Web Enterprise Server (Enterprise Server)* stores distribution kits of anti-virus packages for different OS's of protected computers, updates of virus databases, anti-virus packages and **Enterprise Agents**, user keys and package settings of protected computers. **Enterprise Server** sends necessary information to the correspondent computers on **Agents**' requests and keeps a general log of events of the whole anti-virus network.
- *Dr.Web Control Center* is automatically installed with **Enterprise Server**. It is a certain extension of a web page and allows to administrate the anti-virus network by means of editing the settings of **Enterprise Server** and protected computers stored on **Enterprise Server** and protected computers.
- *Dr.Web Enterprise Agent (Enterprise Agent)* is installed on protected computers. It installs, updates and controls the anti-virus package as instructed by **Enterprise Server**. **Enterprise Agent** reports virus events and other necessary information about the protected computer to **Enterprise Server**.

Optional components:

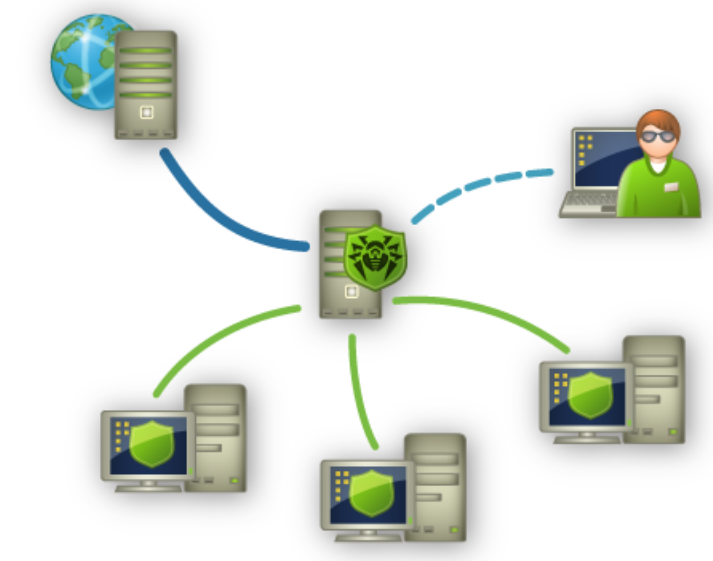
- *Proxy server*. This component can optionally be included into the anti-virus network. The main function of the proxy server is to provide connection between **Enterprise Server** and **Enterprise Agents** in cases when direct connection is impossible. E.g. if the **Server** and **Agents** are located in different networks which do not have packet routing between them. At the expense of using caching function, reducing of network traffic and time of receiving **Agent** updates can be provided.
- *NAP Validator*. Allows to use *Microsoft Network Access Protection (NAP)* technology to check health of **Dr.Web** anti-virus software on protected workstations by enforcing compliance with system health requirements.

The illustration below describes the general scheme of the fragment of the local network where the protecting anti-virus network is organized.



The whole stream of instructions, data and statistics in the anti-virus network always goes through the **Enterprise Server**. **Dr.Web Control Center** exchange information only with **Servers**. Based on **Dr.Web Control Center** commands, **Servers** transfer instructions to **Enterprise Agents** and change the configuration of workstations.

Thus, the logical structure of the fragment of the anti-virus network looks as in the illustration below.



Between the **Server** and workstations (a thin firm line in the illustration) transferring the following information through one of the supported network protocols (TCP, IPX or NetBIOS):

- **Agents'** requests for the centralized schedule and the centralized schedule of workstations,

- settings of the **Agent** and the anti-virus package,
- requests for scheduled tasks to be performed (scanning, updating of virus databases, etc.),
- files of anti-virus packages – when the **Agent** receives a task to install them,
- software and virus databases updates – when an updating task is performed,
- **Agent's** messages on the configuration of the workstation,
- statistics (to be added to the centralized log) on the operation of **Agents** and anti-virus packages,
- messages on virus events and other events which should be logged.

The volume of traffic between the workstations and the **Server** can be quite sizeable subject to the settings and the number of the workstations. Therefore the **Dr.Web ES** provides for the possibility to compress traffic.

Traffic between the **Enterprise Server** and **Enterprise Agent** can be encrypted. This allows to avoid disclosure of data transferred via the described channel as well as to avoid substitution of software downloaded onto workstations.

Thus, Dr.Web ES provides:

- easy centralized installation of the anti-virus SW on protected computers, and in most cases (for computers operated by Windows 2000/XP/Vista) the installation can be done without physical access to a computer;
- centralized set up of the anti-virus SW and update with minimum man-hour spent;
- control of the state of the anti-virus protection;
- centralized launch or termination of tasks of the anti-virus SW on computers (if necessary);
- collection and analysis of information on virus events in all protected computers;
- the option to give some users right to set up the anti-virus SW (if necessary);

- management of the anti-virus network and receipt of information about it by the administrator of the anti-virus protection both from workstations of the corporate network and remotely, from the Internet.

In large corporate networks with hundreds or thousands computers it is advisable to create the **Dr.Web ES** anti-virus network with several **Servers**. The hierarchy connection between the **Servers** allows to simplify the updating of the virus databases and the SW of the workstations and the receipt of the information on the virus events from them. The administrator can analyze the logs of the network, both of separate **Servers** and the summary log of the whole anti-virus network.

Dr.Web ES in corporate networks increases reliability of the anti-virus protection and cuts costs for its administration comparing to installation of personal anti-virus programs on protected computers.

Dr.Web Enterprise Suite has several advantages in comparison to other similar products:

- high reliability and security of applied solutions;
- easy administration;
- multiplatform structure of all components;
- excellent scalability.

We recommend to purchase and install Dr.Web ES if:

- your corporate network has significant size (several dozens of computers or more);
- your network is small, but due to some reasons (determined by the specific SW, equipment or professional skill of the personnel) you already apply the policy of strict administration of installation and set up of a software.

For computers not included into the corporate network use personal anti-viruses – **Dr.Web for Windows** and the **Dr.Web** versions for other platforms.

Appendix F. Dr.Web® AV-Desk for Internet services providers

Dr.Web AV-Desk service is designed on the software-based client-server system, ensures for complete and reliable anti-virus protection of clients workstations of companies specialized in providing various Internet services (Internet providers (ISP), application services providers (ASP), online banking vendors, etc.) provided that the computers are occasionally connected to the Internet.

AV-Desk allows to install **Dr.Web** anti-virus packages for Windows on the workstations of the company's clients, manage their operation, updating, follow up and promptly solve problems, which occur on clients' computers, without the necessity to physically access the workstation or provide support and instructions to the user.

Creating such anti-virus network solves a number of problems, which both corporate clients and individual users often have to face:

- in companies, the software is usually installed onto computers by a company network administrator. The installation of anti-virus programs, their timely updating is an additional work for the administrator and requires physical access to computers;
- at home, users do not always follow up virus events on their computers or may even not install any anti-virus at all;
- semiskilled users can make changes in the settings of the anti-virus (including its disabling because of the seeming inconveniences), which incurs "holes" in protection and thus substantially degrade the level of security;
- anti-virus protection can be fully efficient if its operation is analyzed by qualified specialists, which includes analysis of protocols, files moved to the quarantine, etc. In companies, this work is hampered by the fact that such data is stored in dozens or hundreds computers. At home, operation of the anti-virus once installed is rarely analyzed.

Dr.Web AV-Desk was developed to solve these problems. It provides a reliable, flexible and easy customized anti-virus protection for workstations, saves administrators' time and efforts and relieves users

of the necessity to worry about anti-virus protection, while maintaining a high level of security.

Program solutions used in Dr.Web <%PRODUCT%>, provides for:

- simple installation of software components and prompt arrangement of anti-virus protection,
- creation of distribution files with unique identifiers and their transfer to the users for installation,
- centralized setup of the anti-virus packages,
- centralized virus databases and program files updates on protected computers,
- monitoring of virus events and the state of the anti-virus packages and OS's on all protected computers.

Dr.Web AV-Desk has a *client-server* architecture. **Dr.Web AV-Desk** components are installed on the computers of users and administrators and the computer(s) to function as the **AV-Desk Server**(**s**), and exchange information through network protocols TCP/IP, IPX/SPX, NetBIOS. An aggregate of computers on which **Dr.Web AV-Desk** cooperating components are installed is called an *anti-virus network*.

An anti-virus network includes the following components:

Core components:

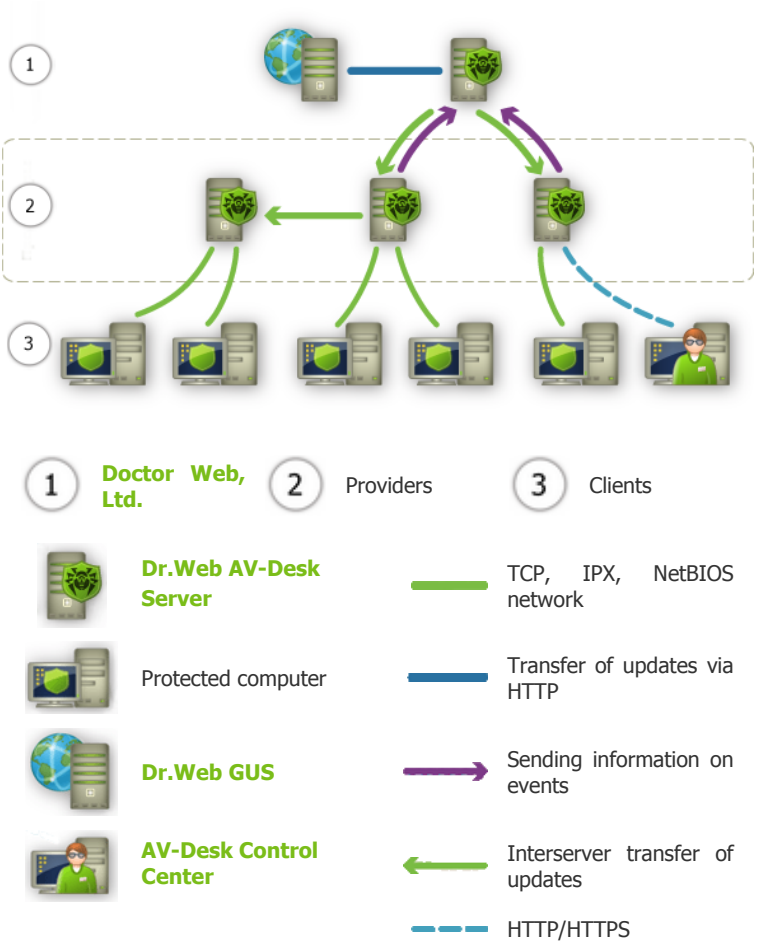
- *Dr.Web AV-Desk Server (AV-Desk Server)* stores distribution kits of anti-virus packages for different OS's of protected computers, updates of virus databases, anti-virus packages and **AV-Desk Agents**, user keys and package settings of protected computers. **AV-Desk Server** sends necessary information to the correspondent computers on **Agents**' requests and keeps a general log of events of the whole anti-virus network.
- *AV-Desk Control Center* is automatically installed with **AV-Desk Server**. It is a certain extension of a web page and allows to administrate the anti-virus network by means of editing the settings of **AV-Desk Server** and protected computers stored on **AV-Desk Server** and protected computers.

- *Dr.Web AV-Desk Agent (AV-Desk Agent)* is installed on protected computers. It installs, updates and controls the anti-virus package as instructed by **AV-Desk Server**. **AV-Desk Agent** reports virus events and other necessary information about the protected computer to **AV-Desk Server**.

Optional components:

- *Proxy server*. This component can optionally be included into the anti-virus network. The main function of the proxy server is to provide connection between **AV-Desk Server** and **AV-Desk Agents** in cases when direct connection is impossible. E.g. if the **Server** and **Agents** are located in different networks which do not have packet routing between them. At the expense of using caching function, reducing of network traffic and time of receiving **Agent** updates can be provided.

The following illustration describes the general scheme of the fragment of the local network where the protecting anti-virus network is organized.



The whole stream of instructions, data and statistics in the anti-virus network always goes through the **AV-Desk Server**. **AV-Desk Control Center** exchange information only with **Servers**. Based on **AV-Desk Control Center** commands, **Servers** transfer instructions to **AV-Desk Agents** and change the configuration of workstations.

In large networks with hundreds or thousands computers it is

advisable to create the **Dr.Web AV-Desk** anti-virus network with several **Servers**. The hierarchy connection between the **Servers** allows to simplify the updating of the virus databases and the SW of the workstations and the receipt of the information on the virus events from them. The administrator can analyze the logs of the network, both of separate **Servers** and the summary log of the whole anti-virus network.

In large networks, **Dr.Web AV-Desk** increases reliability of anti-virus protection and cuts costs for its administration compared personal anti-virus programs.

Dr.Web AV-Desk has several advantages in comparison to other similar products:

- high reliability and security of applied solutions;
- easy administration;
- multiplatform structure of all components;
- excellent scalability.

Appendix G. Technical Support

Support is available to customers who have purchased a commercial version of **Dr.Web** products. Visit **Doctor Web Technical Support** website at http://support.drweb.com/.

If you encounter any issues installing or using company products, take advantage of the following **Doctor Web** support options:

- Download and review the latest manuals and guides at http://download.drweb.com/
- Read the frequently asked questions at http://support.drweb.com/
- Look for the answer in **Dr.Web** knowledge database at http://wiki.drweb.com/
- Browse **Dr.Web** official forum at http://forum.drweb.com/

If you have not found solution for the problem, you can request direct assistance from **Doctor Web Technical Support** by filling in the web-from in the corresponding section of the support site at http://support.drweb.com/.

For regional office information, visit the official **Doctor Web** website at http://company.drweb.com/contacts/moscow

© Doctor Web, 2003-2011